Le frontiere del cybercrime

glossario

PDF generato attraverso il toolkit opensource "mwlib". Per maggiori informazioni, vedi [[http://code.pediapress.com/ http://code.pediapress.com/]].
PDF generated at: Sun, 10 Feb 2013 13:59:10 UTC

Indice

Voci

Cracker 1
Cracking (informatica) 3
Crimine informatico 4
Defacing 11
Exploit 13
Guerra cibernetica 15
Hacker 17
Hacktivism 25
Malware 27
Pharming 30
Phishing 31
Script kiddie 37
Sicurezza informatica 39
Sniffing 47
Spam 51
Spoofing 60
SQL injection 63
Virus (informatica) 65
Warez 74

Note

Fonti e autori delle voci 75
Fonti, licenze e autori delle immagini 76

Licenze della voce

Licenza 77

Cracker

In ambito informatico il termine inglese **cracker** indica colui che si ingegna per eludere blocchi imposti da qualsiasi software al fine di trarne profitto. Il cracking può essere usato per diversi scopi secondari, una volta guadagnato l'accesso di root nel sistema desiderato o dopo aver rimosso le limitazioni di un qualsiasi programma.

I cracker possono essere spinti da varie motivazioni, dal guadagno economico (tipicamente coinvolti in operazioni di spionaggio industriale o in frodi), all'approvazione all'interno di un gruppo di cracker (come tipicamente avviene agli script kiddie, che praticano le operazioni di cui sopra senza una piena consapevolezza né delle tecniche né delle conseguenze).

Il termine cracker viene spesso confuso con quello di hacker, il cui significato è tuttavia notevolmente diverso. Alcune tecniche sono simili, ma hacker è colui che sfrutta le proprie capacità per esplorare, divertirsi, apprendere, senza creare reali danni. Al contrario, cracker è colui che sfrutta le proprie capacità (o in certi casi quelle degli altri) al fine di distruggere (i cracker fanno spesso utilizzo del DoS), ingannare e arricchirsi.

Tipologie di attacco

Nonostante sia molto complesso definire in maniera certa il *modus operandi* del cracker, è possibile grosso modo definire due categorie di attacchi al sistema informatico: l'attacco esterno (remoto) e quello locale.

Attacco esterno

L'attacco esterno ha come finalità:

- lo sfruttamento di una vulnerabilità di un servizio internet, causata da un bug di programmazione (spesso passibili di buffer overflow e simili).
- l'utilizzo di programmi che vengono eseguiti da un server web (cgi-bin) che possono essere utilizzati in modo improprio, ovvero consentono l'esecuzione di comandi oppure soffrono di vulnerabilità analoghe a quelle dei bug dei servizi internet.
- lo sfruttamento di determinate configurazioni insicure dei software web.

Portscanner e security scanner

Per fare questo il cracker si avvale di numerosi software, tra i quali degni di menzione sono i *portscanner* che effettuano dei *port scanning* al fine di individuare quali servizi internet sono attivi su una determinata macchina. I *portscanner* più evoluti sono in grado di determinare anche la versione dei vari software che gestiscono il servizio web. Più evoluti dei *portscanner* sono i *security scanner*, atti a individuare le vulnerabilità dei servizi internet.

Attacco locale

L'attacco locale viene portato a compimento da individui che hanno accesso fisico alla macchina oppure che hanno accesso al sistema via internet tramite delle console remote che permettono loro di eseguire un limitato numero di operazioni con privilegi altrettanto limitati.

Ottenimento di privilegi illimitati

L'ottenimento dello *status* di root, ovvero utente dai privilegi illimitati, si ottiene mediante lo sfruttamento di vulnerabilità di overflow insite nel servizio internet, come descritto nell'attacco esterno, sfruttando difetti nel kernel (solitamente con un attacco locale), la sovrascrittura di file eseguibili o l'utilizzo dei programmi SETUID, che consentono l'esecuzione di determinate operazioni che necessitano di privilegi differenti (solitamente root).

Essere superutente (ovvero root) si rivela essenziale per i cracker che hanno intenzione di nascondere le tracce del proprio passaggio e operare sulla macchina compromessa. Alcune operazioni che solamente root può fare sono ad esempio lo sniffing dei dati in transito su un'interfaccia di rete (solitamente password) e l'utilizzo di software in grado di agire a livello di rete molto basso.

L'eliminazione delle tracce

L'eliminazione delle tracce del proprio passaggio o della propria presenza è essenziale perché il cracker si renda totalmente invisibile all'amministratore di sistema. Ciò viene ottenuto tramite:

- l'eliminazione o modifica dei file di log, che sono i registri che tengono traccia delle operazioni degli utenti
- la modifica dei file eseguibili affinché le operazioni risultino totalmente invisibili
- l'inserimento di codice direttamente all'interno del kernel (in linux tramite dei LKM, moduli caricabili) che modifica e "dirotta" le chiamate di sistema (system call)

Queste operazioni vengono spesso automatizzate e riassunte tramite dei software chiamati rootkit.

Come difendersi

Oggi giorno esistono numerosi sistemi per difendersi e individuare per tempo questi tipi di attacchi.

Il firewall

Il tool più diffuso per proteggere la propria rete o il proprio server è il firewall, che permette di precludere l'accesso a determinati servizi, oppure da un elenco di sistemi che non si ha intenzione di far accedere ai propri servizi internet multimediali.

IDS

Altro software di grande efficacia e complessità è l'Intrusion detection system (IDS) che, attraverso una serie di regole prestabilite rileva tentativi di enumerazione, intrusione o di attacco e li notifica a un operatore.

Voci correlate

- Black hat
- Buffer overflow
- Cracking
- Danneggiamento informatico
- Exploit
- Hacker
- Lamer
- Heap overflow
- Phishing
- Rootkit
- Script kiddie
- Warez

- Spamming
- Ingegneria sociale

Cracker famosi

- Gary McKinnon
- Kevin Mitnick

Cracking (informatica)

Con **cracking** si intende la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata[1]. La distribuzione di software così reso privo di protezione (detto *warez*) è generalmente un'azione illegale a causa della violazione di un copyright. Il *crack* viene spesso ottenuto tramite il reverse engineering, tecnica che permette di capire la logica del software analizzando il suo funzionamento e le risposte a determinati input.

La pratica del cracking esiste da quando esiste il software, ma la modifica del software si è evoluta soprattutto nei primi anni ottanta con la diffusione degli home computer come l'Apple II, l'Atari 80 e il Commodore 64. Con l'evolversi dei computer e dei software, i creatori di crack (detti *cracker*) hanno cominciato a raggrupparsi in squadre, conosciute col nome di "cracking crews". Con la nascita delle *crew* è aumentata notevolmente la competizione già presente tra i crackers, inducendo negli anni una lunga serie di attacchi ai sistemi e lo sviluppo di software come virus e spyware utilizzati per il crack di grandi sistemi informatici.

Per **cracking** si intende anche la violazione di sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (connessione ad Internet, traffico voce, sms, accesso a database etc..) senza la sua autorizzazione (thiefing).

Il termine si contrappone in realtà ad hacking, ma nell'uso comune il termine hacking viene spesso erroneamente utilizzato con il significato di cracking.

Note

[1] Che differenza esiste tra Cracking e Reverse Engineering? (http://quequero.org/UIC_Faq#Che_differenza_c.27.C3.A8_tra_Cracking_e_Reverse_Engineering.3F)

Voci correlate

- Crack (informatica)
- Cracker
- Reverse Engineering
- Sicurezza informatica
- Hexedit

Crimine informatico

Un **crimine informatico** è un fenomeno criminale che si caratterizza nell'abuso della tecnologia informatica sia hardware che software. Alcuni crimini in particolare sono finalizzati allo sfruttamento commerciale della rete[1], a porre a rischio i sistemi informativi di sicurezza nazionale[2].

A livello internazionale, molti governi ed agenzie non governative investono risorse nello spionaggio, nella truffa e in altri crimini transnazionali che coinvolgono interessi economici e politici. La difesa sociale internazionale è impegnata nell'individuare e denunciare tali attori alla Corte Internazionale dell'Aja[3].

Cenni storici

Il crimine informatico può essere generalmente definito come un'attività criminale che coinvolge la struttura della tecnologia di informazione, compreso l'accesso illegale (l'accesso non autorizzato), intercettazione (con mezzi tecnici di trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema informatico), interferenze di dati (danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici), sistemi di interferenza (interferenza con il funzionamento di un sistema informatico mediante l'immissione, trasmissione, danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici), uso improprio di dispositivi, contraffazione (o furto d'identità) e frodi elettroniche.[4]

Le persone che commettono questi crimini, se catturate vengono condannate per l'accusa di aver compiuto reati informatici, come accessi non autorizzati in computer o reti di computer[5].

Agli esordi della sottocultura hacker, le condanne penali erano rare poiché l'approccio degli hacker era rivolto alla conoscenza dei sistemi informatici e della loro sicurezza, pertanto violando i sistemi con azioni non dannose. I sostenitori dell'hacking sono motivati da fini artistici e politici, ma spesso sono indifferenti circa l'uso di mezzi illegali per raggiungerli. Con la crescita dell'industria informatica, sono emersi i casi di violazione dei sistemi informatici per il proprio profitto personale (cracker).

Condanne di reati informatici, o di hacking, iniziarono già nel 1983 con il caso dei *414's* nel Milwaukee. In tal caso, sei adolescenti fecero irruzione in sistemi informatici di prestigio, tra cui il Los Alamos National Laboratory, il Memorial Sloan-Kettering Cancer Center e il Security Pacific Bank. Il 1° Maggio 1983 Gerald Wondra fu condannato a due anni di libertà vigilata.[6] Nel 2006, una pena detentiva di quasi cinque anni è stata tramandata a Jeanson James Ancheta, che ha creato centinaia di computer zombie per eseguire i suoi ordini tramite reti botnet giganti.[7] Egli ha poi venduto le botnet al miglior offerente che a sua volta li ha usati per l'attacco Denial of service.[8]

L'esigenza di punire i crimini informatici emerse già alla fine degli anni ottanta, tanto che, il 13 settembre 1989, il Consiglio d'Europa emanò una *Raccomandazione sulla Criminalità Informatica* dove venivano discusse le condotte informatiche abusive. I reati vennero divisi in due liste: facevano parte della prima lista detta *lista minima* quelle condotte che gli Stati sono invitati a perseguire penalmente quali:

- La frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- Il falso in documenti informatici;
- Il danneggiamento di dati e programmi;
- Il sabotaggio informatico;
- L'accesso abusivo associato alla violazione delle misure di sicurezza del sistema;
- L'intercettazione non autorizzata;
- La riproduzione non autorizzata di programmi protetti;
- La riproduzione non autorizzata di topografie di prodotti a semiconduttore.

Facevano invece parte della seconda lista detta *lista facoltativa* condotte "solo eventualmente" da incriminare, quali:

- L'alterazione di dati o programmi non autorizzata sempre che non costituisca un danneggiamento;
- Lo spionaggio informatico inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- L'utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- L'utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Successivamente, in occasione del XV Congresso dell'Associazione Internazionale di Diritto Penale del 1990, emerse la necessità di incriminare non solo i reati previsti dalla lista minima ma anche le condotte descritte nella lista facoltativa. Le varie legislazioni informatiche che hanno seguito il su detto congresso hanno tenuto conto delle indicazioni date dall'associazione e nel settembre 1994 il Consiglio d'Europa ha aggiornato la precedente Raccomandazione ampliando le condotte perseguibili penalmente, inserendo:

- Il commercio di codici d'accesso ottenuti illegalmente;
- La diffusione di virus e malware.

La più lunga condanna comminata prima del 2012 per reati informatici è quella di Albert Gonzalez per 20 anni.[9]

Le successive condanne più lunghe sono quelle di 13 anni per Max Butler,[10] 108 mesi a Brian Salcedo nel 2004 e confermata nel 2006 dalla Corte d'Appello degli USA,[11][12] e 68 mesi a Kevin Mitnick nel 1999.[13]

L'indirizzo IP non ha valore di prova legale per il principio della responsabilità penale personale e della certezza della norma penale, della pena e della prova (che per il penale non è sufficiente che sia ragionevole, ma deve essere certa). L'indirizzo IP identifica un nodo di rete e non una singola macchina o persona. Infatti, tramite *spoofing* un utente può risultare con un indirizzo IP di una macchina fisicamente anche molto distante, o lo stesso *hardware* può essere condiviso a sua volta da più di un profilo utente.
Logbox è il progetto di un *software* gratuito open-source che l'Unione Europea potrebbe imporre come nativo e parte integrante per la vendita di qualsiasi sistema operativo connesso a Internet: si tratta di un *keylogger*, detto a "scatola nera" perché non può essere modificato o disinstallato nemmeno con privilegi da amministratore di sistema, che traccia qualsiasi azione fatta dall'utente sul PC.

Tipi di reati informatici

Il crimine informatico abbraccia un ampio ventaglio di attività suddivise in due categorie:

- L'utilizzo della tecnologia informatica per compiere l'abuso:
  - Infezione da virus
  - Spam
  - Malware (*malicious code*)
- L'utilizzo dell'elaboratore nella realizzazione del fatto:
  - Cyberstalking
  - Frode e falsa identità
  - Information warfare
  - Phishing

Spam

L'inatteso invio di email per fini commerciali è illegale, ma mentre le leggi anti-spam sono relativamente nuove, le comunicazioni inattese esistono da lungo tempo.

Frode

La *frode informatica* è associata alla frode "tradizionale" con la differenza che è realizzata per mezzo di uno strumento informatico. La legge 547 del 1993 aggiunge al Codice Penale l'art. 640-ter per punire chiunque cerchi di ottenere un arricchimento interferendo abusivamente nell'elaborazione dei dati. Non è identificato come frode informatica l'indebito utilizzo di carte di pagamento magnetiche che è invece disciplinato dall'art. 55 del decreto legislativo 231 del 21 novembre 2007. Altri reati previsti sono:

- La *falsificazione di documenti informatici*. I documenti informatici sono equiparati a tutti gli effetti ai documenti tradizionali e l'art. 491-bis c.p. prevede l'applicabilità delle disposizioni sulla falsità in atti pubblici e privati. La falsificazione in comunicazioni informatiche ricalca invece il delitto di falsità in scrittura privata (art. 485 c.p.).
- Le *aggressioni all'integrità dei dati*. La legge 547 del 1993 amplia le precedenti disposizioni in materia e integra al Codice Penale l'art. 635-bis sul danneggiamento dei sistemi informatici e telematici, l'art. 615-quinquies sulla diffusione di virus e malware, l'art. 392 sulla violenza sulle cose (a tal proposito la legge 547 del 1993 precisa le situazioni dove le aggressioni riguardano beni informatici) ed infine l'art. 420 sul reato di attentato ad impianti di pubblica utilità. Forse l'unico caso giudiziario di diffusione di virus per cui si è celebrato un dibattimento (sia in primo grado, sia in appello) è quello deciso dal Tribunale penale di Bologna con la sentenza 1823/05[14] (la cui decisione è stata parzialmente ribaltata in appello[15]) a proposito del "Caso Vjierika".
- Le *aggressioni alla riservatezza dei dati e delle comunicazioni informatiche*. Riguardo alle forme di intrusione nella sfera privata altrui si incriminano l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), la detenzione o diffusione abusiva di codici di accesso (art. 615-quater c.p.) e la rivelazione del contenuto di documenti segreti (art. 621 c.p.), includendo i documenti protetti contenuti su supporti informatici.

Contenuti sensibili

I contenuti dei siti o altre comunicazioni elettroniche possono essere disattese, oscene od offensive per molte persone, ma non sempre sono illegali. Oltre venticinque paesi pongono dei severi limiti al riguardo comprese le regole per l'emarginazione di utenti che rispondono ai crimini d'odio, alla blasfemia, alla sovversione politica, alla corruzione di minorenni, all'induzione della prostituzione.

La possibilità che queste comunicazioni si diffondano variano da paese a paese e anche all'interno di ogni nazione. Si tratta di un settore dove i Tribunali internazionali possono essere coinvolti per decidere sulle questioni che concernono culture, tradizioni e religioni differenti.

Molestie

Mentre alcuni contentuti possono offendere in maniera indiretta, le molestie informatiche possono colpire la sensibilità di chiunque quali commenti sul genere, etnia, religione e orientamento sessuale. Spesso si verificano nelle chat, nei newsgroup, nelle conferenze virtuali, ecc.

Circa le aggressioni alle comunicazioni informatiche è ampliato il concetto di corrispondenza contenuto nel quarto comma dell'art. 616 c.p. che ingloba anche la corrispondenza informatica e telematica e punisce l'intercettazione e l'interruzione di comunicazioni informatiche (art. 617-quater c.p.) e l'installazione di apparecchiature atte ad intercettare o impedire comunicazioni informatiche (art. 617-quinquies), qualora tali condotte non siano esplicitamente autorizzate.

La legge 48/08[16] che recepisce la Convenzione di Budapest sul crimine informatico ha modificato il codice penale e quello di procedura penale riconoscendo implicitamente il ruolo dell'informatica forense nel processo penale[17].

Spaccio di sostanze illecite

I trafficanti di droga stanno ottenendo vantaggi economici tramite messaggi criptati e altre tecnologie virtuali. Gli acquirenti frequentano determinati locali come, ad es., i coffe shop o i milk bar utilizzando siti web finti allo scopo di individuare intere partite di pillole e quantità di anfetamine in chat room.

L'aumento dello spaccio via internet potrebbe essere attribuito alla carenza di comunicazioni dirette in modo da stimolare qualsiasi persona ad acquistare la droga. Gli effetti che sono spesso associati allo spaccio di droga, infatti, sono minimizzati e filtrati dai processi che intervengono dall'interazione virtuale.

Terrorismo

Agenti governativi e di sicurezza hanno registrato un sensibile incremento dei problemi virtuali sin dal 2001. Ma c'è una buona parte di coloro che ritengono le intrusioni come parte di un disegno terroristico più grande.

Un terrorista informatico, quindi, è un individuo o un gruppo di soggetti che, tramite l'attacco informatico, la rete o l'acquisizione segreta di informazioni, ricatta o pone in pericolo un governo o un'azienda al fine di ottenere qualcosa in contropartita per raggiungere i propri fini criminali.

Ad es., una innocente propaganda su internet su una fantomatica bomba che esploderà durante un evento o un periodo di tempo, può essere considerato alla stregua di terrorismo informatico. Allo stesso modo, ci sono delle attività illegali dirette verso individui, famiglie, organizzazioni, che tendono a causare panico tra la gente, squilibrare rapporti di forza, raccogliere informazioni rilevanti per la salute della popolazione ed altri simili sconvolgimenti.

L'estorsione informatica, in particolare, è una forma di terrorismo informatico nella quale un sito, un'email o un server è soggetto a ripetuti attacchi da parte di hackers al fine di ottenere denaro. Seguendo l'FBI, l'estorsione informatica è in aumento nei confronti di aziende e servizi privati, nella media di venti casi al mese, che si trovano costretti a sborsare milioni di dollari pena l'irrimediabile perdita di tutti i propri dati e sistemi informatici[18].

Diritto d'autore

Nei casi di pirateria informatica, è punita l'appropriazione indebita dell'idea originale. Gli oggetti che si intende tutelare sono di diversi tipi.

- Le topografie. Con qualche anno di ritardo rispetto ai termini previsti dalla direttiva europea, la legge 70 del 21 febbraio 1989 tutela le topografie di prodotti a semiconduttori ovvero i tracciati incisi sulle piastrine di silicio. A tal proposito non sono previste sanzioni penali per le violazioni dei diritti nonostante la Raccomandazione del 13 settembre 1989 del Consiglio d'Europa le preveda.
- I software. Con la modifica della legge 633 del 22 aprile 1941 sul diritto d'autore, i programmi per elaboratore vengono inclusi tra le opere di ingegno. In seguito alla Direttiva CEE del 14 maggio 1991 recepita dal Dlgs 518 del 29 dicembre 1992, si vuole prevenire la duplicazione e la vendita dei programmi a fine di lucro (art. 171-bis 1.a.). La sanzione pecuniaria prevista è successivamente aggravata dal Dlgs 205 del 15 marzo 1996.
- I database. Il Dlgs 169 del 6 maggio 1999 riconosce i diritti di esclusiva al creatore del database (artt 64-quinquies e sexies) e il diritto di tutela al "costitutore" del database, ovvero a colui che effettua investimenti in termini di tempo e denaro per raccogliere e inserire materiale nel database, con il fine di salvaguardare il valore patrimoniale dell'investimento.
- Le opere fonografiche e videografiche. Gli abusi di duplicazione e distribuzione vengono disciplinati dalla legge 406 del 29 luglio 1981, mentre le opere cinematografiche destinate al circuito cinematografico e televisivo sono tutelate dalla legge 400 del 20 luglio 1985.
- Le modifiche hardware a consolle per videogiochi sono state fatte rientrare, dalla giurisprudenza, nell'ambito della tutela del diritto d'autore. In giurisprudenza è ancora aperto il dibattito sulla legittimità dei modchip, da quando il Tribunale penale di Bolzano, con la sentenza 20 dicembre 2005[19], li ritenne legali, ma altri tribunali si dimostrarono di avviso contrario.

Guerre informatiche

Il Department of Defense americano evidenzia che il crimine informatico ha assunto forme che coinvolgono le strategie di politica globale. Nel 2007 si sono verificati degli attacchi contro il sistema informatico dell'Estonia da parte di hackers di origine russa. Analogamente nel 2008 la Russia ha denunciato attacchi da parte dei terroristi ceceni. Nel timore che questi attacchi possano prefigura l'estensione del conflitto di più ampia portata, le forze di spionaggio militare si sono da tempo attivate per predisporre strategie tese ad individuare i campanelli di allarme e prevenire conflitti in futuro[20].

Criminalistica

Uno dei più celebri casi di crimine informatico si è verificato per tre volte a partire dal 1970 quando la New York's Union Dime Savings Bank si è appropriata indebitamente di oltre 1 milione di dollari da centinaia di conti correnti[21].

Un'organizzazione di hacker denominata " Masters of Deception" ha rubato migliaia di password dalle compagnie telefoniche così come dei codici di carte di credito a disposizione di diverse università per un ammontare di oltre 370000$[21].

Nel 1983 uno studente ultranovantenne era riuscito ad entrare nel sistema informatico del Dipartimento di Difesa del Pentagono e a scaricare alcune informazioni riservate[21].

Tra il 1995 e il 1998 il satellite Newscorp utilizzato dal canale Sky di Rupert Murdoch è stato ripetutamente manipolato da un gruppo di hacker per trasmettere la serie di Star Trek in alcuni paesi, come la Germania, dove, tra l'altro, Sky non aveva la licenza di trasmettere[22].

Nel febbraio 2000 un soggetto che si nascondeva dientro il nickname "MafiaBoys" effettuò una serie di attacchi contro siti molto frequentati quali Yahoo!, Amazon.com, Dell, Inc., E-Trade, eBay, and CNN. Circa cinquanta PC alla Stanford University sono stati utilizzati per compiere attacchi DdoS. Il 3 agosto 2000, la polizia canadese ha scoperto il "MafiaBoys" che, al momento dell'arresto, aveva con sé oltre 54 account ilelgali, oltre ad una dozzina di account per mascherare la propria identità.

Il Russian Business Network è stata registrata nel World Wide Web fin dal 2006 e, almeno inizialmente, la sua attività sembrava del tutto legale. Poi col passare del tempo, gli organizzatori si sono resi conto che era molto più conveniente collezionare attività illegali ed iniziarono ad avere contatti con la mafia russa offrendo hosting e accesso ad internet a molti noti criminali per un giro di affari di oltre 150 milioni di dollari all'anno[23].

Il 2 marzo 2010 gli investigatori spagnoli scoprirono un'infezione da virus avvenuta in oltre 13 milioni di PC incluse molte aziende, banche ed altri enti finanziari.

Nell'agosto 2010 il Department of Homeland Security scoprì un giro internazionale di pedofilia con circa 600 affiliati che hanno contribuito a diffondere oltre 123 terabyte di materiale pedopornografico (equivalente a circa 16000 DVD). Al momento si tratta del dato peggiore registrato dall'autorità giudiziaria[24].

Prospettive sul crimine informatico

Le tipologie di reato in Internet sono di svariati tipi: dal messaggio offensivo inviato per posta elettronica, alla diffusione di immagini diffamatorie o pedopornografiche, o al download di risorse protette dal diritto d'autore. L'identificazione dell'autore di un reato online è resa problematica da molteplici fattori: in un sistema, quale Internet, non controllato da alcuna autorità sovranazionale che consente agli utenti l'assoluto anonimato, dove i dati si diffondono con rapidità elevatissima oltre i confini nazionali, e dove cancellare le tracce è relativamente semplice, identificare il responsabile di un reato è un'operazione davvero complessa che difficilmente è eseguita con successo.

Note

[1] Mann and Sutton 1998: >>Netcrime: More change in the Organization of Thieving. British Journal of Criminology; 38: 201-229. Oxfordjournals.org (http://bjc.oxfordjournals.org/cgi/content/abstract/38/2/201)

[2] Internet Security Systems. March-2005.

[3] Ophardt, Jonathan A. "Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield" (http://www.law.duke.edu/journals/dltr/articles/2010dltr003.html) *Duke Law and Technology Review*, February 23, 2010.

[4] Paul Taylorwkautore, *Hackers: Crime in the Digital Sublime*, November 3, 1999[a] ed., Routledge; 1 edition, pp. 200. ISBN 0-415-18072-4

[5] Bruce Sterlingwkautore Bruce Sterling, *The Hacker Crackdown—Law and Disorder on the Electronic Frontier*, January 1994[a] ed., Project Gutenberg, 1993, pp. 336. ISBN 0-553-56370-X

[6] *Computer User Sentenced* (http://query.nytimes.com/gst/fullpage.html?res=9F01E2D71338F932A35756C0A962948260), May 1, 1983. URL consultato in data September 11, 2008.

[7] pg 26—Richard Gisselwkautore, *Digital Underworld*, August 23, 2005[a] ed., Lulu, pp. 222. ISBN 1-4116-4423-9

[8] Robert Vamosi. *Cybercrime does pay; here's how* (http://reviews.cnet.com/4520-3513_7-6427016-1.html). CNET Reviews, January 27, 2006. URL consultato in data September 11, 2008.

[9] Kim Zetter. *TJX Hacker Gets 20 Years in Prison* (http://www.wired.com/threatlevel/2010/03/tjx-sentencing/), Wired (magazine), March 25, 2010. URL consultato in data January 22, 2012.

[10] Kevin Poulsen. *Record 13-Year Sentence for Hacker Max Vision* (http://www.wired.com/threatlevel/2010/02/max-vision-sentencing/), Wired (magazine), February 12, 2010. URL consultato in data January 22, 2012.

[11] *Hacker Sentenced to Prison for Breaking into Lowe's Companies' Computers with Intent to Steal Credit Card Information* (http://www.cybercrime.gov/salcedoSent.htm). cybercrime.gov, December 15, 2004. URL consultato in data January 22, 2012.

[12] *Crazy-Long Hacker Sentence Upheld* (http://www.wired.com/science/discoveries/news/2006/07/71358), Wired (magazine), July 11, 2006. URL consultato in data January 22, 2012.

[13] *Kevin Mitnick Sentenced to Nearly Four Years in Prison* (http://www.cybercrime.gov/mitnick.htm). cybercrime.gov, August 9, 1999. URL consultato in data January 22, 2012.

[14] Sentenza 1823/05 del Tribunale penale di Bologna (http://www.ictlex.net/?p=516)

[15] C. App. Bologna, Sent. 369/08 (http://www.ictlex.net/?p=692)

[16] legge 48/08 (http://www.ictlex.net/?p=599)

[17] Fonte: Come cambia la legge sui reati informatici - PC Professionale n. 205 aprile 2008 (http://www.ictlex.net/?p=605)

[18] Lepofsky, J. (2006, June). Cyberextortion by denial-of-service attack. Risk, Retrieved from http://www.ere-security.ca/PDF/Cyberextortion%20by%20DoS,%20Risk%20Magazine%20June%202006.pdf

[19] sentenza 20 dicembre 2005 del Tribunale penale di Bolzano (http://www.ictlex.net/?p=527)

[20] "War is War? The utility of cyberspace operations in the contemporary operational environment" (http://www.carlisle.army.mil/DIME/documents/War is War Issue Paper Final2.pdf) U.S. Army War College, February 2010.

[21] Ronald Weitzer, *Current Controversies in Criminology*, Upper Saddle River, New Jersey, Pearson Education Press, 2003, pp. 150.

[22] Mann, D. and Sutton, M. (1998) >>Netcrime: More Change in the Organization of Thieving. British Journal of Criminology. 38:PP. 201-229 Oxfordjournals.org (http://bjc.oxfordjournals.org/cgi/content/short/38/2/201)

[23] *A walk on the dark side* (http://economist.com/displaystory.cfm?story_id=9723768). The Economist, 30 settembre 2007

[24] DHS: Secretary Napolitano and Attorney General Holder Announce Largest U.S. Prosecution of International Criminal Network Organized to Sexually Exploit Children (http://www.dhs.gov/ynews/releases/20110803-napolitano-holder-announce-largest-prosecution-criminal-network.shtm)

Bibliografia

- Aterno S., Cajani F., Costabile G, Mattiucci M., Mazzaraco G. (2011) *Computer Forensics e Indagini Digitali. Manuale Tecnico-Giuridico e Casi Pratici* (http://www.telematici.com)*", Experta.*
- Balkin J., et al., (2006) (eds) *Cybercrime: Digital Cops in a Networked Environment*, New York University Press, New York.
- Brenner S. (2007) *Law in an Era of Smart Technology,* Oxford: Oxford University Press
- Cajani F., Costabile G., Mazzaraco G. (2008) *Phishing e furto d'identità digitale* (http://www.giuffre.it/it-IT/products/133947.html), Milano, Giuffrè.
- Csonka P. (2000) *Internet Crime; the Draft council of Europe convention on cyber-crime: A response to the challenge of crime in the age of the internet?*, "Computer Law & Security Report", Vol.16 no.5.
- Cuniberti M., Gallus G.B., Micozzi F.P. (2009) *I nuovi reati informatici* (http://www.giappichelli.it/home/978-88-7524-158-2,7524158.asp1), Torino, Giappichelli.
- Easttom C. (2010) *Computer Crime Investigation and the Law*

- Fafinski S. (2009) *Computer Misuse: Response, regulation and the law* Cullompton: Willan
- Grabosky P. (2006) *Electronic Crime,* New Jersey: Prentice Hall
- *United Nations Manual on the prevention and control of computer-related crime*, "International review of criminal policy", 1999, 43-44.
- McQuade S. (2006) *Understanding and Managing Cybercrime,* Boston: Allyn & Bacon.
- McQuade S. (2009) *The Encyclopedia of Cybercrime,* Westport, CT: Greenwood Press.
- Parker D. (1983) *Fighting Computer Crime,* U.S.: Charles Scribner's Sons.
- Pattavina A. (ed.) *Information Technology and the Criminal Justice System,* Thousand Oaks, CA: Sage.
- Paul Taylor, *Hackers: Crime in the Digital Sublime*, November 3, 1999, Routledge; 1 edition, pp. 200. ISBN 0415180724
- Robertson J. (2010). *Authorities bust 3 in infection of 13m computers* (http://www.boston.com/business/technology/articles/2010/03/02/authorities_bust_3_in_infection_of_13m_computers/), Retrieved March 26, 2010, from Boston News.
- Santoriello C., et al., (2010) *I reati informatici. Nuova disciplina e tecniche processuali di accertamento* (http://books.google.it/books?id=ed9QiczvzkkC&dq=cybercrime&source=gbs_navlinks_s), Milano, Wolters Kluwer Italia.
- Walden I. (2007) *Computer Crimes and Digital Investigations*, Oxford: Oxford University Press.
- Wall D.S. (2007) *Cybercrimes: The transformation of crime in the information age,* Cambridge: Polity.
- Williams M. (2006) *Virtually Criminal: Crime, Deviance and Regulation Online,* Routledge, London.
- Yar M. (2006) *Cybercrime and Society,* London: Sage.

Voci correlate

- Criminalità organizzata
- Criminalità organizzata transnazionale
- Cyberbullismo
- Diritto informatico
- Garante per la protezione dei dati personali
- Guerra cibernetica
- Metasploit Project
- Misure minime di sicurezza
- Partito Pirata
- Privacy
- Sicurezza informatica
- Spionaggio industriale

Altri progetti

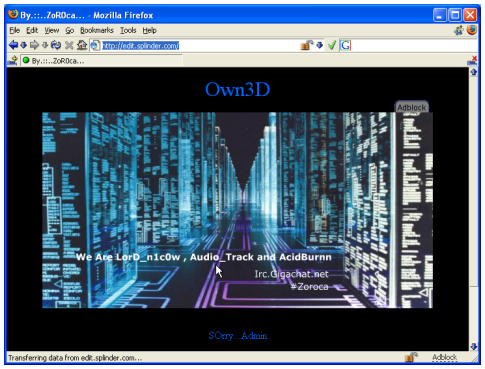
- **Wikisource** contiene opere originali: http://it.wikisource.org/wiki/Puoi_fidarti_del_tuo_computer%3F
- **Wikibooks** contiene testi o manuali: http://it.wikibooks.org/wiki/Crittografia
- **Wikiversità** contiene informazioni: http://it.wikiversity.org/wiki/Servizi_di_sicurezza_nelle_reti_IP:_IPSec,_SSL,_TLS
- **Wikinotizie** contiene notizie di attualità: http://it.wikinews.org/wiki/Gli_hacker_cinesi_violano_anche_i_siti_del_governo_inglese

Collegamenti esterni

- Anti Phishing Italia (http://www.anti-phishing.it/)
- Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (http://www.poliziadistato.it/articolo/view/18494/)
- Computer Crime Guide (http://legal.practitioner.com/computer-crime/)
- Computer Crime Research Center (http://www.crime-research.org)
- Crimine.info (http://www.crimine.info/)
- Crimini informatici (http://www.carabinieri.it/Internet/Cittadino/Consigli/Tematici/Internet/02_internet.htm)
- Cybercrime.gov (http://www.cybercrime.gov/)
- Cybercrimes.it (http://www.cybercrimes.it/)
- FBI Cyber Investigations home page (http://www.fbi.gov/cyberinvest/cyberhome.htm)
- Polizia postale (http://poliziadistato.it/articolo/982/)
- Procura della Repubblica presso il Tribunale di Milano - *pool* reati informatici (http://www.procura.milano.giustizia.it/reati-informatici.html)
- Unità di analisi sul crimine informatico (http://www.poliziadistato.it/articolo/986/)
- Wikileaks Italia (http://www.wikileaksitalia.org/)
- (**EN**) Crimine informatico (http://www.wikiartpedia.org/index.php?title=Concerning_Hackers_Who_Break_into_Computer_Systems) su WikiARTpedia
- (**EN**) Hacker High: 10 Stories of Teenage Hackers Getting into the System (http://www.itsecurity.com/features/hacker-high-061008/)
- (**EN**) CUSSE List of Convicted Hackers (http://cusse.org/rogues)

Defacing

Defacing (termine inglese che, come il suo sinonimo ***defacement***, ha il significato letterale di "sfregiare, deturpare,sfigurare", in italiano reso raramente con **defacciare**) nell'ambito della sicurezza informatica ha solitamente il significato di cambiare illecitamente la home page di un sito web (la sua "faccia") o modificarne, sostituendole, una o più pagine interne. Pratica che, condotta da parte di persone non autorizzate e all'insaputa di chi gestisce il sito, è illegale in tutti i paesi del mondo.



esempio di defacing di un sito

Un sito che è stato oggetto di questo tipo di *deface* vede sostituita la propria pagina principale, spesso insieme a tutte le pagine interne, con una schermata che indica l'azione compiuta da uno o più cracker. Le motivazioni di tale atto vandalico possono essere di vario tipo, dalla dimostrazione di abilità a ragioni ideologiche. Le tecniche utilizzate per ottenere i permessi di accesso in scrittura al sito sfruttano solitamente i bug presenti nel software di gestione del sito oppure nei sistemi operativi sottostanti; più raro il caso di utilizzo di tecniche di ingegneria sociale.

Aspetti legali

Legge italiana

In Italia il *defacing* si traduce in tre tipi di reato grave previsti dal Codice Penale, quelli di accesso abusivo ad un sistema informatico e di diffamazione:

- Art. 615 Ter (Accesso abusivo ad un sistema telematico o informatico): *"Chiunque abusivamente si introduca in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantenga contro la volontà espressa o tacita di chi ha il diritto di escluderlo è punito con la pena della reclusione fino a tre anni."*
- Art 635 bis (Danneggiamento di sistemi informatici e telematici): *Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*

  Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".
- Art. 595 (Diffamazione) : *Chiunque comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino ad un anno o con la multa sino a lire due milioni (circa 1032 €).*

  Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a lire quattro milioni (circa 2065 €).

  Se l'offesa è arrecata col mezzo della stampa, o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a lire un milione (circa 516 €)."

Leggi più severe sarebbero in fase di studio.

Tipi di defacing

In base alle motivazioni che stanno alla base dell'esecuzione, i tipi di *defacing* possono essere svariati. Tra questi vi sono:

- Truffa: un cracker cambia la pagina del sito in cui esiste il link per una immissione di una carta di credito o similari, reindirizzandola verso una pagina personale allo scopo di carpire le informazioni che consentiranno, ad esempio, il prelievo illegale di denaro.
- Propaganda: un hacker cambia in parte o tutto la pagina di un sito ideologicamente avverso per screditarlo o denigrarlo.
- Controllo occulto: la polizia inserisce degli elementi di controllo, per sapere quanti utenti accedono alla pagina del sito, per ottenere elementi utili alla loro identificazione e/o, talvolta, scoraggiarli facendo apparire scritte intimidatorie o facendo cadere la connessione dopo alcuni tentativi.
- Spamming: si inseriscono ben evidenti elementi pubblicitari, come dei link a siti commerciali.
- Ricatto: minacciando di perpetrare ripetuti defacing, si tenta di ricattare i proprietari del sito a scopo di estorsione o altro.
- Burla: soprattutto (ma non esclusivamente) da parte dei più giovani, si cambia la pagina inserendo frasi o richiami infantili del tipo "pippo è stato qua" (vedi: lamer).
- Come avviso per far notare al webmaster che il sito è vulnerabile ed è stato bucato.

Modalità

Per poter modificare le pagine di un sito web è necessario recuperare le password di accesso al sito, oppure riuscire ad avere i permessi di scrittura in altro modo.

Esistono inoltre tool che hanno interessato il Wikiwiki di GPI, occupando d'inviare routine di semplici messaggi POST o GET alla pagina, che non è protetta, inserendo bug.

R57

L'R57 è una shell usata dai defacer per effettuare defacing sfruttando una vulnerabilità del sito, in molti casi è il Remote File Inclusion (inclusione di file remoto).

Viene usata anche per molti altri usi come caricare processi tipo ircbot, rxbot, e altri processi per fare dosnet e botnet. L'altra shell "gemella" della r57 è la c99 usata per i medesimi scopi ma molto più amichevole e facile da usare.

Voci correlate

- Accesso abusivo ad un sistema informatico o telematico
- Danneggiamento informatico
- SQL injection

Exploit

Un **exploit** è un termine usato in informatica per identificare un codice che, sfruttando un bug o una vulnerabilità, porta all'acquisizione di privilegi o al denial of service di un computer.

Descrizione

Ci sono diversi modi per classificare gli exploit. Il più comune è una classificazione a seconda del modo in cui l'exploit contatta l'applicazione vulnerabile. Un *exploit remoto* è compiuto attraverso la rete e sfrutta la vulnerabilità senza precedenti accessi al sistema. Un *exploit locale* richiede un preventivo accesso al sistema e solitamente fa aumentare i privilegi dell'utente oltre a quelli impostati dall'amministratore.

Gli exploit possono anche essere classificati a seconda del tipo di vulnerabilità che sfruttano. Vedi buffer overflow, Heap Overflow, format string attacks, race condition, double free(), Integer overflow, SQL injection, cross-site scripting, cross-site request forgery, remote file inclusion e local file inclusion.

Lo scopo di molti exploit è quello di acquisire i privilegi di root su un sistema. È comunque possibile usare exploit che dapprima acquisiscono un accesso con i minimi privilegi e che poi li alzano fino ad arrivare a root.

Normalmente un exploit può sfruttare solo una specifica falla, e quando questa falla viene riparata, l'exploit diventa inutile per le nuove versioni del programma. Per questo motivo alcuni blackhat hacker non divulgano gli exploit trovati ma li tengono riservati per loro o per la loro comunità. Questi exploit sono chiamati *zero day exploit*, e scoprire il loro contenuto è il più grande desiderio per gli attacker senza conoscenze, altrimenti detti script kiddie. Gli exploit più sfruttati sono scritti in Perl, C e PHP

Voci correlate

- Arbitrary code execution
- Shellcode
- Sicurezza informatica
- Virus

Collegamenti esterni

- (**EN**) Milw0rm [1] il più grande archivio di exploit del web
- (**EN**) World Wide Exploits Database by K-OTik Security [2] in inglese - richiesta registrazione
- (**EN**) Metasploit Framework [3] in inglese
- (**EN**) Rosiello Security Exploits [4] in inglese
- (**EN**) Advanced Exploit Tutorials [5] in inglese
- (**EN**) Proof of concept exploit downloads [6] in inglese
- (**EN**) Home of the Bugtraq exploit mailing list [7] in inglese
- (**EN**) ExploitTree [8] from SecurityForest [9] in inglese

Note

[1] http://www.milw0rm.com/
[2] http://www.k-otik.com/exploits/
[3] http://www.metasploit.com/projects/Framework/
[4] http://www.rosiello.org/
[5] http://medialab.freaknet.org/~alpt/tutorial/papers.html
[6] http://www.packetstormsecurity.org
[7] http://www.securityfocus.com/
[8] http://www.securityforest.com/wiki/index.php/Category:ExploitTree
[9] http://www.securityforest.com/

Guerra cibernetica

Il termine **guerra cibernetica**[1] (noto nell'ambito operativo militare del mondo anglofono come *cyberwarfare*) è l'insieme delle attività di preparazione e conduzione delle operazioni militari eseguite nel rispetto dei principi bellici condizionati dall'informazione. Si traduce nell'alterazione e addirittura nella distruzione dell'informazione e dei sistemi di comunicazioni nemici, procedendo a far sì che sul proprio fronte si mantenga un relativo equilibrio dell'informazione. La guerra cibernetica si caratterizza per l'uso di tecnologie elettroniche, informatiche e dei sistemi di telecomunicazione.

Tipi di attacchi

Esistono molte metodologie di attacco nella guerra cibernetica, la lista seguente è ordinata dalla più lieve alla più pericolosa.[2]

- **Vandalismo Web**: Attacchi volti a "sporcare" pagine web o per mettere fuori uso i server (attacchi denial-of-service). Normalmente queste aggressioni sono veloci e non provocano grandi danni.
- **Propaganda**: Messaggi politici che possono essere spediti a coloro che sono collegati alla Rete.
- **Raccolta dati**: le informazioni riservate ma non protette possono essere intercettate e modificate, rendendo possibile lo spionaggio.
- **Distruzione delle apparecchiature** (Equipment disruption): attività militari che utilizzano computer e satelliti per coordinarsi sono potenziali vittime di questi attacchi. Ordini e comunicazioni possono essere intercettati o sostituiti, mettendo a rischio i soldati.
- **Attacco a infrastrutture critiche**: I servizi energetici, idrici, di combustibili, di comunicazioni, commerciali e dei trasporti sono tutti vulnerabili a questo genere di attacchi.

Attacchi conosciuti

- Gli Stati Uniti d'America hanno ammesso di essere stati sotto attacco da parte di diversi Stati, ad esempio Cina e Russia. I due attacchi più famosi sono passati alla storia con i nomi di Titan Rain e Moonlight Maze. [3]

Regole base

Le regole base della cyberwarfare sono:

- minimizzare la spesa di capitali e di energie produttive e operative;
- sfruttare appieno tecnologie che agevolino le attività investigative e di acquisizione di dati, l'elaborazione di questi ultimi e la successiva distribuzione dei risultati ai comandanti delle unità operative;
- ottimizzare al massimo le comunicazioni tattiche, i sistemi di posizionamento e l'identificazione amico-nemico (IFF - "Identification Friend or Foe").

Organizzazione

Con la cyberwarfare si conosce un radicale riassetto delle concezioni organizzative militari. Le tradizionali strutture gerarchiche si vedono progressivamente soppiantate da sistemi a rete, con nuovi ruoli di complementarità e integrazione. Si fanno così spazio entità operative caratterizzate da:

- ridotta consistenza numerica;
- elevato livello di supporto tecnologico;
- efficacia assoluta.

Controspionaggio cyberspaziale

Il controspionaggio cyberspaziale è l'insieme delle misure atte a identificare, penetrare o neutralizzare operazioni straniere che usano i mezzi cyber come metodologie di attacco primario, così come gli sforzi dei servizi stranieri di intelligence che, attraverso l'uso di metodi tradizionali, cercano di portare avanti attacchi di cyberwarfare.[4]

Note

[1] Cfr. in Riccardo Busetto, *Il dizionario militare: dizionario enciclopedico del lessico militare*, Bologna, 2004, Zanichelli, ISBN 9788808089373

[2] (**EN**) Tipi di cyber-warfare (http://www.tecsoc.org/natsec/focuscyberwar.htm)

[3] (**EN**) [[Reuters (http://www.propagandamatrix.com/articles/november2006/031106_b_cyberspace.htm)]: L'U.S. Air Force si prepara a combattere nel cyberspazio]

[4] (**EN**) DOD - Controspionaggio cyberspaziale (http://www.dtic.mil/doctrine/jel/doddict/data/c/01472.html)

Bibliografia

- Maddalena Oliva, *Fuori Fuoco. L'arte della guerra e il suo racconto*, Bologna, Odoya 2008. ISBN 978-88-6288-003-9.
- Daniel Ventre, *La guerre de l'information*, Hermès-Lavoisier, Sept.2007.
- Daniel Ventre, *Information Warfare*, Wiley-ISTE, Nov. 2009.
- Daniel Ventre, *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Hermès-Lavoisier, Sept.2010.
- Daniel Ventre, *Cyberespace et acteurs du cyberconflit*, Hermès-Lavoisier, April 2011.
- Daniel Ventre, *Cyberwar and Information Warfare*, Wiley-ISTE, July 2011.
- Daniel Ventre, *Cyberattaque et Cyberdéfense*, Hermès Lavoisier, August 2011.

Voci correlate

- Sicurezza informatica
- Armi a impulso elettromagnetico
- Guerra elettronica
- ELINT
- Spionaggio
- High Energy Radio Frequency weapons (HERF)
- SIGINT
- Hacker warfare
- Operazione Aurora

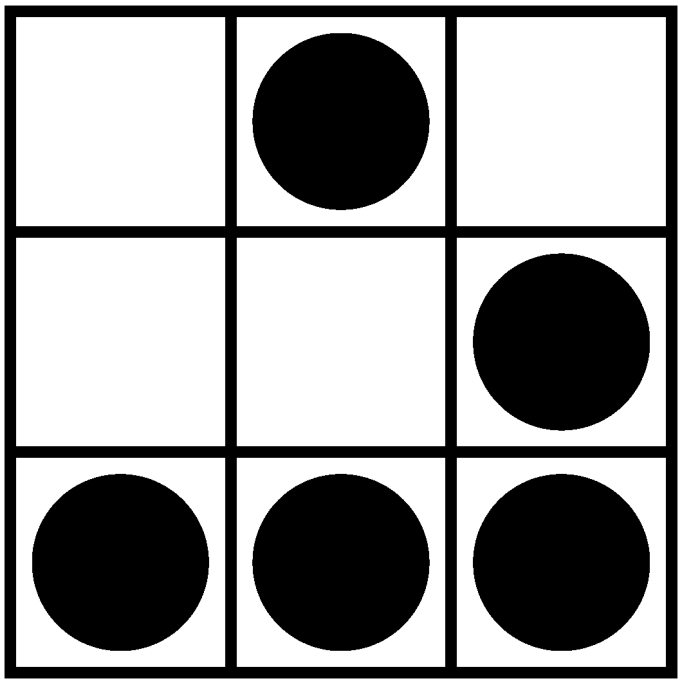
Collegamenti esterni

- (EN) Cyberwarfare 'a reality in 12 months' (http://news.zdnet.co.uk/internet/security/0,39020375,39119111,00.htm)
- (EN) Iraq's Crash Course in Cyberwar (http://www.wired.com/news/conflict/0,2100,58901,00.html)
- (EN) Special focus on cyber-warfare (http://www.tecsoc.org/natsec/focuscyberwar.htm)
- (EN) U.S. Air Force prepares to fight in cyberspace (http://www.cnn.com/2006/TECH/internet/11/03/airforce.cyberspace.reut/index.html)
- Cyberwarfare e Cyberspace: aspetti concettuali, fasi ed applicazione allo scenario nazionale ed all'ambito militare (CeMiSS) (http://www.difesa.it/SMD/CASD/Istituti_militari/CeMISS/Pubblicazioni/News206/2008-01/Pagine/Cyberwarfare_e_Cyberspace_aspet_9342militare.aspx)

Hacker

Un **hacker** (termine coniato negli Stati Uniti d'America che si può rendere in italiano con *smanettone*) è una persona che si impegna nell'affrontare sfide intellettuali per aggirare o superare creativamente le limitazioni che gli vengono imposte, non limitatamente ai suoi ambiti d'interesse (che di solito comprendono l'informatica o l'ingegneria elettronica), ma in tutti gli aspetti della sua vita.

Esiste un luogo comune, usato soprattutto dai mass media (a partire dagli anni ottanta), per cui il termine hacker viene associato ai criminali informatici, la cui definizione corretta è, invece, "cracker".



Il "glider", simbolo per identificare gli hacker, proposto da Eric S. Raymond[1]

Origine del termine

Il New Hacker Dictionary, compendio online dove sono raccolti i termini gergali dei programmatori, elenca ufficialmente nove diverse connotazioni per la parola "hack" e un numero analogo per "hacker". Eppure la stessa pubblicazione include un saggio d'accompagnamento in cui si cita Phil Agre, un hacker del Massachusetts Institute of Technology (MIT) che mette in guardia i lettori a non farsi fuorviare dall'apparente flessibilità del termine. "*Hack ha solo un significato*" - sostiene Agre - "*Quello estremamente sottile e profondo di qualcosa che rifiuta ulteriori spiegazioni.*"

A prescindere dall'ampiezza della definizione, la maggioranza degli odierni hacker ne fa risalire l'etimologia al MIT, dove il termine fece la sua comparsa nel gergo studentesco all'inizio degli anni cinquanta. Secondo una pubblicazione diffusa nel 1990 dal MIT Museum, a documentare il fenomeno dell'hacking, per quanti frequentavano l'istituto in quegli anni il termine "hack" veniva usato con un significato analogo a quello dell'odierno "*goof*" (*scemenza*, *goliardata*). Stendere una vecchia carcassa fuori dalla finestra del dormitorio veniva considerato un

"hack", ma altre azioni più pesanti o dolose - ad esempio, tirare delle uova contro le finestre del dormitorio rivale, oppure deturpare una statua nel campus - superavano quei limiti. Era implicito nella definizione di "hack" lo spirito di un divertimento creativo e innocuo.

È a tale spirito che s'ispirava il gerundio del termine: "hacking". Uno studente degli anni cinquanta che trascorreva gran parte del pomeriggio chiacchierando al telefono o smontando una radio, poteva descrivere quelle attività come "hacking". Di nuovo, l'equivalente moderno per indicare le stesse attività potrebbe essere la forma verbale derivata da "*goof*" - "*goofing*" o "*goofing off*" (prendere in giro qualcuno, divertirsi).

Più avanti negli anni cinquanta, il termine "hack" acquistò una connotazione più netta e ribelle. Al MIT degli anni cinquanta vigeva un elevato livello di competizione e l'attività di hacking emerse sia come reazione sia come estensione di una tale cultura competitiva. Goliardate e burle varie divennero tutt'a un tratto un modo per scaricare la tensione accumulata, per prendere in giro l'amministrazione del campus, per dare spazio a quei pensieri e comportamenti creativi repressi dal rigoroso percorso di studio dell'istituto. Va poi aggiunto che quest'ultimo, con la miriade di corridoi e tunnel sotterranei, offriva ampie opportunità esplorative per quegli studenti che non si facevano intimorire da porte chiuse e da cartelli tipo "Vietato l'ingresso". Fu così che "*tunnel hacking*" divenne l'accezione usata dagli stessi studenti per indicare queste incursioni sotterranee non autorizzate. In superficie il sistema telefonico del campus offriva analoghe opportunità. Grazie ad esperimenti casuali ma accurati, gli studenti impararono a fare scherzi divertenti. Traendo ispirazione dal più tradizionale "tunnel hacking", questa nuova attività venne presto battezzata "phone hacking", per poi diventare l'odierno phreaking.

La combinazione tra divertimento creativo ed esplorazioni senza limiti costituirà la base per le future mutazioni del termine hacking. I primi ad auto-qualificarsi "computer hacker" nel campus del MIT negli anni sessanta traevano origine da un gruppo di studenti appassionati di modellismo ferroviario, che negli ultimi anni cinquanta si erano riuniti nel *Tech Model Railroad Club*. Una ristretta enclave all'interno di quest'ultimo era il comitato *Signals and Power* (segnali ed elettricità) - gli addetti alla gestione del sistema del circuito elettrico dei trenini del club. Un sistema costituito da un sofisticato assortimento di relè e interruttori analogo a quello che regolava il sistema telefonico del campus. Per gestirlo era sufficiente che un membro del gruppo inviasse semplicemente i vari comandi tramite un telefono collegato al sistema, osservando poi il comportamento dei trenini.

Bruce Sterling autore del libro Giro di vite contro gli hacker

I nuovi ingegneri elettrici responsabili per la costruzione e il mantenimento di tale sistema considerarono lo spirito di simili attività analogo a quello del phone hacking. Adottando il termine hacking, iniziarono così a raffinarne ulteriormente la portata. Dal punto di vista del comitato *Signals and Power*, usare un relè in meno in un determinato tratto di binari significava poterlo utilizzare per qualche progetto futuro. In maniera sottile, il termine hacking si trasformò da sinonimo di gioco ozioso, a un gioco in grado di migliorare le prestazioni o l'efficienza complessiva del sistema ferroviario del club. Quanto prima i membri di quel comitato cominciarono a indicare con orgoglio l'attività di ricostruzione e miglioramento del circuito per il funzionamento delle rotaie con il termine "hacking", mentre "hacker" erano quanti si dedicavano a tali attività.

Considerata la loro affinità per i sistemi elettronici sofisticati - per non parlare della tradizionale avversione degli studenti del MIT verso porte chiuse e divieti d'ingresso - non ci volle molto prima che gli hacker mettessero le mani su una macchina appena arrivata al campus. Noto come TX-0, si trattava di uno dei primi modelli di computer lanciati sul mercato. Sul finire degli anni cinquanta, l'intero comitato *Signals and Power* era emigrato in massa nella

sala di controllo del TX-0, portandosi dietro lo stesso spirito di gioco creativo. Il vasto reame della programmazione informatica avrebbe portato a un ulteriore mutamento etimologico. "To hack" non indicava più l'attività di saldare circuiti dalle strane sembianze, bensì quella di comporre insieme vari programmi, con poco rispetto per quei metodi o procedure usati nella scrittura del software "ufficiale". Significava inoltre migliorare l'efficienza e la velocità del software già esistente che tendeva a ingolfare le risorse della macchina. Ed è qui che successivamente si colloca una diversa radice del termine hacker, la forma sostantiva del verbo inglese "to hack" che significa "tagliare", "sfrondare", "sminuzzare", "ridurre", "aprirsi un varco", appunto fra le righe di codice che istruiscono i programmi software. Un hacker era quindi uno che riduceva la complessità e la lunghezza del codice sorgente, con un "hack", appunto, una procedura grossolana ma efficace, che potrebbe essere tradotta in italiano come "zappata" o "accettata" (tagliata con l'accetta) o altrimenti con una "furbata". Rimanendo fedele alla sua radice, il termine indicava anche la realizzazione di programmi aventi l'unico scopo di divertire o di intrattenere l'utente, come "scrivere numeri romani" (cit. Richard Stallman).

Spacewar!

Un classico esempio di quest'ampliamento della definizione di hacker è Spacewar!, il primo video game interattivo. Sviluppato nei primi anni sessanta dagli hacker del MIT, Spacewar! includeva tutte le caratteristiche dell'hacking tradizionale: era divertente e casuale, non serviva ad altro che a fornire una distrazione serale alle decine di hacker che si divertivano a giocarvi. Dal punto di vista del software, però, rappresentava una testimonianza incredibile delle innovazioni rese possibili dalle capacità di programmazione. Inoltre era completamente libero (e gratuito). Avendolo realizzato per puro divertimento, gli hacker non vedevano alcun motivo di mettere sotto scorta la loro creazione, che finì per essere ampiamente condivisa con altri programmatori. Verso la fine degli anni sessanta, Spacewar! divenne così il passatempo preferito di quanti lavoravano ai mainframe in ogni parte del mondo.

Furono i concetti di innovazione collettiva e proprietà condivisa del software a distanziare l'attività di computer hacking degli anni sessanta da quelle di tunnel hacking e phone hacking del decennio precedente. Queste ultime tendevano a rivelarsi attività condotte da soli o in piccoli gruppi, per lo più limitate all'ambito del campus, e la natura segreta di tali attività non favoriva l'aperta circolazione di nuove scoperte. Invece i computer hacker operavano all'interno di una disciplina scientifica basata sulla collaborazione e sull'aperto riconoscimento dell'innovazione. Non sempre hacker e ricercatori "ufficiali" andavano a braccetto, ma nella rapida evoluzione di quell'ambito le due specie di programmatori finirono per impostare un rapporto basato sulla collaborazione - si potrebbe perfino definire una relazione simbiotica.

Richard Stallman

Il fatto che la successiva generazione di programmatori, incluso Richard Stallman, aspirasse a seguire le orme dei primi hacker, non fa altro che testimoniare le prodigiose capacità di questi ultimi. Nella seconda metà degli anni settanta il termine "hacker" aveva assunto la connotazione di *élite*. In senso generale, computer hacker era chiunque scrivesse il codice software per il solo gusto di riuscirci. In senso specifico, indicava abilità nella programmazione. Al pari del termine "artista", il significato conteneva delle connotazioni tribali. Definire hacker un collega programmatore costituiva un segno di rispetto. Auto-descriversi come hacker rivelava un'enorme fiducia personale. In entrambi i casi, la genericità iniziale dell'appellativo computer hacker andava diminuendo di pari passo alla maggiore diffusione del computer.

Con il restringimento della definizione, l'attività di computer hacking acquistò nuove connotazioni semantiche. Per potersi definire hacker, una persona doveva compiere qualcosa di più che scrivere programmi interessanti; doveva

far parte dell'omonima cultura e onorarne le tradizioni allo stesso modo in cui un contadino del Medio Evo giurava fedeltà alla corporazione dei vinai. Pur se con una struttura sociale non così rigida come in quest'ultimo esempio, gli hacker di istituzioni elitarie come il MIT, Stanford e Carnegie Mellon iniziarono a parlare apertamente di "etica hacker": le norme non ancora scritte che governavano il comportamento quotidiano dell'hacker. Nel libro del 1984 "Hackers. Gli eroi della rivoluzione informatica", l'autore Steven Levy, dopo un lungo lavoro di ricerca e consultazione, codificò tale etica in cinque principi fondamentali.

Sotto molti punti di vista, i principi elencati da Levy continuano a definire l'odierna cultura del computer hacking. Eppure l'immagine di una comunità hacker analoga a una corporazione medievale, è stata scalzata dalle tendenze eccessivamente populiste dell'industria del software. A partire dai primi anni ottanta i computer presero a spuntare un po' ovunque, e i programmatori che una volta dovevano recarsi presso grandi istituzioni o aziende soltanto per aver accesso alla macchina, improvvisamente si trovarono a stretto contatto con hacker di grande livello via ARPANET. Grazie a questa vicinanza, i comuni programmatori presero ad appropriarsi delle filosofie anarchiche tipiche della cultura hacker di ambiti come quello del MIT. Tuttavia, nel corso di un simile trasferimento di valori andò perduto il tabù culturale originato al MIT contro ogni comportamento malevolo, doloso. Mentre i programmatori più giovani iniziavano a sperimentare le proprie capacità con finalità dannose - creando e disseminando virus, facendo irruzione nei sistemi informatici militari, provocando deliberatamente il blocco di macchine quali lo stesso Oz del MIT, popolare nodo di collegamento con ARPAnet - il termine "hacker" assunse connotati punk, nichilisti. Quando polizia e imprenditori iniziarono a far risalire quei crimini a un pugno di programmatori rinnegati che citavano a propria difesa frasi di comodo tratte dall'etica hacker, quest'ultimo termine prese ad apparire su quotidiani e riviste in articoli di taglio negativo. Nonostante libri come quello di Levy avessero fatto parecchio per documentare lo spirito originale di esplorazione da cui nacque la cultura dell'hacking, per la maggioranza dei giornalisti "computer hacker" divenne sinonimo di "rapinatore elettronico". Contro l'originale definizione da questo momento si insinua nella conoscenza popolare l'uguaglianza Hacker-Malvivente.

Anche di fronte alla presenza, durante gli ultimi due decenni, delle forti lamentele degli stessi hacker contro questi presunti abusi, le valenze ribelli del termine risalenti agli anni cinquanta rendono difficile distinguere tra un quindicenne che scrive programmi capaci di infrangere le attuali protezioni cifrate, dallo studente degli anni sessanta che rompe i lucchetti e sfonda le porte per avere accesso a un terminale chiuso in qualche ufficio. D'altra parte, la sovversione creativa dell'autorità per qualcuno non è altro che un problema di sicurezza per qualcun altro. In ogni caso, l'essenziale tabù contro comportamenti dolosi o deliberatamente dannosi trova conferma a tal punto da spingere la maggioranza degli hacker ad utilizzare il termine cracker - qualcuno che volontariamente decide di infrangere un sistema di sicurezza informatico per rubare o manomettere dei dati - per indicare quegli hacker che abusano delle proprie capacità.

Questo fondamentale tabù contro gli atti dolosi rimane il primario collegamento culturale esistente tra l'idea di hacking del primo scorcio del XXI secolo e quello degli anni cinquanta. È importante notare come, mentre la definizione di computer hacking abbia subìto un'evoluzione durante gli ultimi quattro decenni, il concetto originario di hacking in generale - ad esempio, burlarsi di qualcuno oppure esplorare tunnel sotterranei - sia invece rimasto inalterato. Nell'autunno 2000 il MIT Museum onorò quest'antica tradizione dedicando al tema un'apposita mostra, la Hall of Hacks. Questa comprendeva alcune fotografie risalenti agli anni venti, inclusa una in cui appare una finta auto della polizia. Nel 1993, gli studenti resero un tributo all'idea originale di hacking del MIT posizionando la stessa macchina della polizia, con le luci lampeggianti, sulla sommità del principale edificio dell'istituto. La targa della macchina era IHTFP, acronimo dai diversi significati e molto diffuso al MIT e attualmente la stessa macchina è esposta all'interno dell'edificio del MIT, Ray and Maria Stata Center. La versione maggiormente degna di nota, anch'essa risalente al periodo di alta competitività nella vita studentesca degli anni cinquanta, è "*I hate this fucking place*" (Odio questo fottuto posto). Tuttavia nel 1990, il Museum riprese il medesimo acronimo come punto di partenza per una pubblicazione sulla storia dell'hacking. Sotto il titolo "*Institute for Hacks Tomfoolery and Pranks*" (Istituto per scherzi folli e goliardate), la rivista offre un adeguato riassunto di quelle attività.

"*Nella cultura dell'hacking, ogni creazione semplice ed elegante riceve un'alta valutazione come si trattasse di scienza pura*", scrive Randolph Ryan, giornalista del Boston Globe, in un articolo del 1993 incluso nella mostra in cui compariva la macchina della polizia. "*L'azione di hack differisce da una comune goliardata perché richiede attenta pianificazione, organizzazione e finezza, oltre a fondarsi su una buona dose di arguzia e inventiva. La norma non scritta vuole che ogni hack sia divertente, non distruttivo e non rechi danno. Anzi, talvolta gli stessi hacker aiutano nell'opera di smantellamento dei propri manufatti*".

A questo proposito all'ingresso del MIT Ray and Maria Stata Center è presente un cartello intitolato "Hacking Ethics" che riporta 11 punti a cui dovrebbe rifarsi ogni hacker. Questi sono:

1. Be safe. Your safety, the safety of your fellow jackers, and the safety of anyone you hack should never be compromised.
2. Be subtle. Leave no evidence that you were ever there.
3. Leave things as you found them (or better).
4. If you find something broken, call F-IXIT (the local number for reporting problems wit the buildings and grounds). Hackers often go places that institute workers do not frequent regularly and may see problems before anyone else.
5. Leave no damage.
6. Do not steal anything.
7. Brute force is the last resort of the incompetent. ("One who breaks a thing to find out what it is has left the path of reason." - John Ronald Reuel Tolkien, "The Lord of the Rings")
8. Do not hack while under the influence of alcohol/drugs/etc.
9. Do not drop things (off a building) without ground crew.
10. Do not hack alone (just like swimming).
11. Above all, exercise common sense.

Inoltre, sempre all'ingresso del MIT, è presente un altro cimelio della storia dell'hacking proprio accanto ai "comandamenti" dell'etica di un Hacker: L'idrante del MIT [2] collegato a una fontana indicante la famosa frase del presidente del MIT Jerome Weisner (1971-1980) "Getting an education at MIT is like taking a drink from a fire hose", ovvero, "Assimilare un'educazione al MIT è come bere da un tubo antincendio".

Il desiderio di confinare la cultura del computer hacking all'interno degli stessi confini etici appare opera meritevole ma impossibile. Nonostante la gran parte dell'hacking informatico aspiri al medesimo spirito di eleganza e semplicità, il medium stesso del software offre un livello inferiore di reversibilità. Smontare una macchina della polizia è opera semplice in confronto allo smantellamento di un'idea, soprattutto quando è ormai giunta l'ora per l'affermazione di tale idea. Da qui la crescente distinzione tra "black hat" e "white hat" ("cappello nero" e "cappello bianco") - hacker che rivolgono nuove idee verso finalità distruttive, dolose contro hacker che invece mirano a scopi positivi o, quantomeno, informativi.

Una volta oscuro elemento del gergo studentesco, la parola "hacker" è divenuta una palla da biliardo linguistica, soggetta a spinte politiche e sfumature etiche. Forse è questo il motivo per cui a così tanti hacker e giornalisti piace farne uso. Nessuno può tuttavia indovinare quale sarà la prossima sponda che la palla si troverà a colpire.

Un "*h4x0r*" (pronuncia "achs-or") è il termine hacker scritto in leet (linguaggio degli hacker).

Significati

Volendo specificare tutti i vari ambiti in cui viene usato il termine "hacker", si possono evidenziare questi significati:

1. Qualcuno che conosce la programmazione abbastanza bene da essere in grado di scrivere un software nuovo e utile senza troppa fatica, in una giornata o comunque rapidamente.
2. Qualcuno che riesce ad inserirsi in un sistema o in una rete per aiutare i proprietari a prendere coscienza di un problema di sicurezza. Anche detti "white hat hacker" o "sneaker". Molte di queste persone sono impiegate in aziende di sicurezza informatica e lavorano nella completa legalità. Gli altri vengono definiti "black hat hacker" sebbene spesso il termine venga connotato anche in maniera più negativa del semplice "aiutare i proprietari" e collegato al vero e proprio vandalismo.
3. Qualcuno che, attraverso l'esperienza o per tentativi successivi, modifica un software esistente in modo tale da rendere disponibile una nuova funzione. Più che una competizione, lo scambio tra diversi programmatori di modifiche sui relativi software è visto come un'occasione di collaborazione.
4. Un "Reality Hacker" o "Urban Spelunker" (origine: MIT) è qualcuno che si addentra nei meandri più nascosti di una città, spesso mettendo a segno "scherzi" elaborati per il divertimento della comunità.

Un Hacker in senso stretto è colui che associa ad una profonda conoscenza dei sistemi una intangibilità dell'essere, esso è invisibile a tutti eccetto che a sé stesso. Non sono certamente Hacker in senso stretto tutti coloro che affermano di esserlo, in un certo senso gli Hacker in senso stretto non esistono, perché se qualcuno sapesse della loro esistenza per definizione non esisterebbero.

"*Script kiddie*" è un termine che indica un utente con poca o nessuna cultura informatica che segue semplicemente delle istruzioni o un "cook-book" senza capire il significato di ciò che sta facendo. Spesso viene utilizzato per indicare chi utilizza exploit creati da altri programmatori e hacker.

Un "*lamer*" è uno script kiddie che utilizza ad esempio trojan (NetBus, subseven) per pavoneggiarsi con gli altri e far credere di essere molto esperto, ma in realtà non sa praticamente nulla e si diverte ad arrecare danno ad altri. I Lamer sono notoriamente disprezzati dagli Hacker appunto per la loro tendenza a danneggiare gratuitamente i computer e successivamente a vantarsi di quello che hanno fatto.

Un "*newbie*" (niubbo) è una persona alle prime armi in questo campo.

Hacker famosi

- Richard Greenblatt e Bill Gosper - programmatori, considerati i fondatori della comunità hacker nella prima parte degli anni 1960
- Richard Stallman - programmatore (autore, tra gli altri, di Emacs e GCC), ideatore del concetto di Software libero e di copyleft
- Ward Cunningham - ideatore del concetto di wiki
- Johan Helsingius - mantenne il più famoso anonymous remailer del mondo, finché non lo chiuse nel 1996
- Eric S. Raymond - fondatore del movimento open source, scrittore di libri e saggi sulla cultura hacker
- Tsutomu Shimomura - avversario del famoso cracker Kevin Mitnick, che riuscì a far arrestare
- Ken Thompson e Dennis Ritchie - autori del sistema operativo Unix
- Linus Torvalds - autore del Kernel Linux
- Larry Wall - autore del Perl
- Tron - abile phreaker tedesco morto in modo misterioso
- John Draper - Meglio conosciuto come Capitan Crunch, primo phreaker della storia
- Loyd Blankenship - Meglio conosciuto come The Mentor. Scrittore del breve saggio *The Hacker Manifesto*, considerato una pietra miliare della cultura hacker
- George Francis Hotz - È stato il primo a violare la sicurezza della PlayStation 3, è diventato famoso con alcuni tool da lui sviluppati per il Jailbreak dell'Iphone

- Rafael Núñez - noto anche come RaFa (...), hacker venezuelano, membro dei World of Hell
- Adrian Lamo
- Anonymous
- Steve Wozniak
- Robert Morris
- Gary McKinnon (hacker) anche noto come "Solo" È accusato dalla giustizia statunitense di aver perpetrato "la più grande intrusione informatica su computer appartenenti alla difesa che si sia mai verificata in tutti i tempi."
- Jono Bacon
- Raffaele Forte È il fondatore e principale sviluppatore del progetto Linux BackBox
- Ingo Molnar è un programmatore e hacker ungherese attualmente impiegato presso la Red Hat
- Fredrik Neij alias TiAMO (27 aprile 1978), è un hacker svedese. È co-fondatore di The Pirate Bay
- Georg C. F. Greve È il fondatore e presidente della Free Software Foundation Europe
- Bradley M. Kuhn è un programmatore e hacker statunitense.
- Benjamin Mako Hill È un collaboratore dei progetti Debian e Ubuntu e sviluppatore di software libero
- William John Sullivan
- Onel de Guzmán
- Ricardo Galli è un programmatore e hacker spagnolo
- Kevin Mitnick alias "Condor" è stato uno degli hacker più abili degli anni '90. Si è distinto nella sua vita per azioni di phreaking, hacking, cracking, ingegneria sociale. Ha violato diverse banche dati di grandi corporations americane. E' inventore dell'IP spoofing. Ricercato e catturato nel 1995, si è fatto 5 anni di carcere dopo aver tenuto in scacco le polizie degli USA per molti anni. Ora si occupa di sicurezza informatica.

Filmografia

- *Codice Swordfish* (*Swordfish*) (2001)
- *Hackers* (1995)
- *I pirati di Silicon Valley* (*Pirates of Silicon Valley*) (1999)
- *I signori della truffa* (*Sneakers*) (1992)
- *Takedown* (*Track Down*) (2000)
- *The Net - Intrappolata nella rete* (*The Net*) (1995)
- *Wargames - Giochi di guerra* (*WarGames*) (1983)
- *Wargames 2 - Il codice della paura* (*Wargames: The Dead Code*) (2008)
- *The Net 2.0* (*The Net 2.0*) (2006)
- *S.Y.N.A.P.S.E. - Pericolo in rete* (*Antitrust*) (2001)
- *Firewall - Accesso negato* (Firewall) (2006)

Bibliografia

- Stefano Chiccarelli, Andrea Monti, *Spaghetti hacker*, 2011, Monti & Ambrosini Editori, ISBN 978-88-89479-14-8
- Steven Levy, *Hackers. Gli eroi della rivoluzione informatica*, 1999, Shake Editore, ISBN 88-86926-97-9
- Carlo Gubitosa, *Italian crackdown. BBS amatoriali, volontari telematici, censure e sequestri nell'Italia degli anni '90* [3], Apogeo, 1999. ISBN 9788873035299 URL consultato il 2010-07-03.
- Steven Levy, *Crypto, i ribelli del codice in difesa della privacy*, 2002, Shake Editore, ISBN 88-86926-81-2
- Arturo Di Corinto, Tommaso Tozzi, *Hacktivism. La libertà nelle maglie della rete*, 2002, Manifestolibri, ISBN 88-7285-249-8
- Sam Williams, *Codice libero*, 2002, ISBN 88-503-2108-2
- Raoul Chiesa, *Hacking e Criminalità*, 2002

- Pekka Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*, 2003, ISBN 88-078-1745-4
- Bruce Sterling, *Giro di vite contro gli hacker*, 2004, ISBN 88-045-2387-5
- Anna Fici, *Mondo hacker e logica dell'azione collettiva*, 2004, ISBN 88-464-5935-0
- McKenzie Wark, *Un manifesto hacker*, 2005, ISBN 88-071-7108-2
- *Ippolita* [4], *Open non è free* [5]. Comunità digitali tra etica hacker e mercato globale, Eleuthera, 2005, ISBN 8889490047
- Luca Carettoni, David Laniado, *Etica Hacker: l'imperativo è hands-on* [6], 2005, Politecnico di Milano
- Carlo Gubitosa, *Elogio della pirateria. Dal Corsaro Nero agli hacker, dieci storie di ribellioni creative* [7], Terre di Mezzo, 2005. ISBN 9788889385371 URL consultato il 2010-07-03.
- Carlo Gubitosa, *Hacker, scienziati e pionieri. Storia sociale del ciberspazio e della comunicazione elettronica* [8], Viterbo, Stampa Alternativa, 2007. ISBN 9788872269732 URL consultato il 2010-07-03.

Voci correlate

- Cracker
- Hacking
- Accesso abusivo ad un sistema informatico o telematico
- Hackmeeting
- Pwn2Own
- Hacklab
- Hackerspace
- Massachusetts institute of technology
- Jargon File
- Software libero
- Ingegneria sociale
- Black hat
- White hat
- Geo spoofing
- The Tao of Programming
- Operazione Payback

Note

[1] *The Glider: A Universal Hacker Emblem* (http://www.catb.org/hacker-emblem/). catb.org, 3 dicembre 2006. URL consultato in data 30-12-2007.

[2] http://4.bp.blogspot.com/-Tjouyfgiohw/UMSoQ3xh40I/AAAAAAAAAV0/9Gii-185kxs/s1600/IMG_0726.jpg

[3] http://www.apogeonline.com/openpress/libri/529/index.html

[4] http://www.ippolita.net/

[5] http://www.ippolita.net/onf/

[6] http://airwiki.ws.dei.polimi.it/images/4/46/Hackdoc.pdf

[7] http://www.stampalternativa.it/liberacultura/books/elogio_pirateria.pdf

[8] http://www.stampalternativa.it/liberacultura/?p=156

Altri progetti

- **Wikizionario** contiene la voce di dizionario: http://it.wiktionary.org/wiki/hacker
- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Hackers
- **Wikiquote** contiene citazioni: http://it.wikiquote.org/wiki/Hacker

Collegamenti esterni

- (EN) The IHTFP Gallery - Sito Ufficiale degli Hacks dell' MIT (http://hacks.mit.edu/)
- (EN) Il New Hacker Dictionary (http://catb.org/jargon/html/index.html)
- (EN) How to become an Hacker (http://www.catb.org/~esr/faqs/hacker-howto.html) di Eric S. Raymond
- (EN) Proposta per il simbolo degli hacker (http://www.catb.org/~esr/hacker-emblem/)

Hacktivism

Hacktivism è un termine che deriva dall'unione di due parole, hacking e *activism* e indica le pratiche dell'azione diretta digitale in stile hacker.

Nell'ambito della filosofia hacktivist, le forme dell'azione diretta tradizionale sono trasformate nei loro equivalenti elettronici: la manifestazione di piazza, il corteo, si è trasformata nel netstrike, il corteo telematico; l'occupazione di stabili in disuso, nel cybersquatting; il volantinaggio all'angolo delle strade nell'invio massivo di e-mail di partecipazione e di protesta, il banchetto delle petizioni nelle petizioni on line; i tazebao scritti a mano diventano pagine web e le scritte sui muri e i graffiti vengono sostituiti dal defacciamento temporaneo di siti web. In omaggio all'etica primigenia dell'hacking, gli hacktivisti agiscono mettendo a disposizione di tutti risorse informative e strumenti di comunicazione. Le pratiche hacktivist si concretizzano nella realizzazione di server indipendenti e autogestiti per offrire servizi di mailing list, e-mail, spazi web, ftp server, sistemi e database crittografici, circuiti di peer to peer, archivi di video e foto digitali, webradio.

Origine del termine

Il termine è stato coniato nelle interazioni fra i protagonisti delle prime azioni di disobbedienza civile in rete. In particolare è stato riferito agli autori dei primi netstrike condotti a livello mondiale per protestare contro abusi dei diritti civili, governi corrotti o sentenze di pena di morte. Successivamente il termine hacktivism è stato impiegato per indicare le pratiche di coloro i quali, usando reti e computer in modo creativo, hanno messo in discussione l'operato di governi e multinazionali organizzando petizioni online, virus benevoli, siti web di controinformazione, e altri strumenti per l'abilitazione di tutti i cittadini alla libera comunicazione elettronica.

Controversie

Sono in molti a ritenere che pratiche digitali come il mailbombing e il defacciamento dei siti, ma anche la realizzazione di virus e malware siano in disaccordo con l'etica hacker di facilitare l'accesso all'informazione in tutte le sue forme e quindi contrarie all'etica hacktivist che punta a promuovere la consapevolezza dell'importanza dell'informazione e della comunicazione come agenti di cambiamento sociale.

Bibliografia

- Luca Cian (a cura di), *Comunicazione liberata. Altri modi di comunicare e partecipare* , Brioschi Editore, 2011. ISBN 9788895399638
- (con Alessandro Gilioli), Arturo Di Corinto *I nemici della rete* , BUR-Biblioteca Universale Rizzoli, 2010 ISBN 9788817042758

- AA. VV., *La privatizzazione della vita. Brevetti, monopoli, multinazionali* , Punto Rosso, 2004. ISBN 9788883510410
- (con Arianna Dagnino) Gulmanelli Stefano *Popwar. Il Netattivismo contro l'ordine costituito* , Apogeo, 2003. ISBN 8850321554
- Matteo Pasquinelli (a cura di), *Media Activism: Strategie e pratiche della comunicazione indipendente* , Roma: Derive Approdi, 2002. ISBN 88-87423-87-3
- (con Tommaso Tozzi) Arturo Di Corinto, *Hacktivism. La libertà nelle maglie della rete* , Manifestolibri, 2002, ISBN 8872852498
- AA. VV., *La sfida al G8* , Manifestolibri, 2001, ISBN 8872851920

Voci correlate

- Jewish Internet Defense Force

Collegamenti esterni

- Hacktivism. La libertà nelle maglie della rete [1]
- La Sfida al G8 [2].

Collegamenti esterni in lingua inglese

- Hacktivist.net [3] Popular site of hacktivist opinions and information
- Hacktivism in the Culture Jammers Encyclopedia [4]
- Hacktivismo's Projects Page [5]
- Hacktivism and the Future of Political Participation [6] Political science dissertation on the history and political significance of hacktivism
- Hack This Site! Hacktivist training ground [7]
- Hackbloc [8] Home of the hacktivist zine "HackThisZine"
- What is Hacktivism? [9]
- White Hat, Black Hat, Grey Hat links [10]
- Surveillance, Free Speech and Privacy in the Electronic Age [11]
- Hacktivism information and discussions [12]
- Hacktivism in the context of body modification [13] (usage coined by Lukas Zpira)

Note

[1] http://www.hackerart.org/storia/hacktivism.htm
[2] http://www.manifestolibri.it/vedi_brano.php?id=272
[3] http://www.hacktivist.net
[4] http://www.sniggle.net/hacktivism.php
[5] http://www.hacktivismo.com/projects/
[6] http://www.alexandrasamuel.com/dissertation/pdfs/index.html
[7] http://www.hackthissite.org
[8] http://www.hackbloc.org
[9] http://thehacktivist.com/hacktivism.php
[10] http://www.wbglinks.net
[11] http://www.libertes-internets.net
[12] http://www.hacktivism.info/index.php
[13] http://wiki.bmezine.com/index.php/Hacktivism

Malware

Nella sicurezza informatica il termine **malware** indica genericamente un qualsiasi software creato con il solo scopo di causare danni più o meno gravi ad un computer, ai dati degli utenti del computer, o a un sistema informatico su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malvagio"; in italiano è detto anche *codice maligno*.

La diffusione di tali software risulta in continuo aumento: si calcola che nel solo anno 2008 su Internet siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti, e tali numeri sono destinati verosimilmente ad aumentare con l'espansione della Rete e il progressivo diffondersi della cultura informatica.[1]

Interfaccia di Beast, un trojan categoria backdoor che colpisce il sistema operativo Windows

Categorie di malware

Si distinguono molte categorie di malware, anche se spesso questi programmi sono composti di più parti interdipendenti e rientrano pertanto in più di una classe. Vista inoltre la rapida evoluzione in questo campo, la classificazione presentata di seguito non è da ritenersi esaustiva.

- Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.
- Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.
- Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla

connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.
- Rootkit: i rootkit solitamente sono composti da un driver e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare *spyware* e *trojan*.
- Scareware: sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.
- Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.
- Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.
- Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altre cose dannose) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità. Bisogna però anche dire che esistono modi per camuffare i Batch e farli sembrare dei file exe, aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" è spesso ricorrente nel Cyberbullismo.
- Keylogger: I Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i keylogger vengono installati sul computer dai trojan o dai worm, in altri casi invece il keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente.
- Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.
- Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.

Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e l'equivoco viene alimentato dal fatto che gli antivirus permettono di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Si noti che un malware è caratterizzato dall'intento doloso del suo creatore, dunque non rientrano nella definizione data i programmi contenenti bug, che costituiscono la normalità anche quando si sia osservata la massima diligenza nello sviluppo di un software.

Attività criminose legate ai malware

La legislazione relativa ai malware è estremamente variabile a seconda delle nazioni ed è in continua evoluzione. In generale se i *virus*, i *worm* e i *trojan* sono illegali in quasi ogni parte del mondo non si può dire lo stesso per le altre categorie. I *dialer* in particolare sono di per sé legali, tanto che ogni sistema operativo moderno ne contiene almeno uno. L'ambiguità è peggiorata dal fatto che molti software si situano sul limite che separa un vero e proprio malware da un programma forse fastidioso ma non dannoso.

Attualmente i malware (in particolare *trojan*, *worm*, *spyware* e malware) vengono utilizzati per inviare grandi quantità di file non richiesti dall'utente; quest'ultimi vengono solitamente venduti agli spammer. Esiste un vero e proprio mercato nero legato ai malware: oltre alla compravendita di dati personali, è possibile acquistare *l'utilizzo* di computer infetti, cioè la possibilità di impiegare, per i propri fini e a insaputa dei legittimi proprietari, una certa quantità (nell'ordine delle migliaia) di computer controllati da remoto tramite una *backdoor*.

Note

[1] Dati riferiti in un rapporto diffuso da Panda Security (http://www.pandasecurity.com/italy/) e riportati in *Sicurezza, in una classifica i bug più pericolosi* (punto-informatico.it) (http://punto-informatico.it/2523404/PI/News/sicurezza-una-classifica-bug-piu-pericolosi.aspx)

Voci correlate

- Backdoor
- Bomba logica
- Dialer
- Grayware
- Mousetrapping
- Rootkit
- Spyware
- Stacheldraht
- Trojan
- Virus
- Worm
- Malwarebytes' Anti-Malware

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Malware

Collegamenti esterni

- (**EN**) Un articolo (http://www.washingtonpost.com/wp-dyn/content/article/2006/02/14/AR2006021401342.html) del Washington Post sullo sfruttamento commerciale del malware.
- Malicious Software (http://www.dmoz.org/Computers/Security/Malicious_Software/) su Open Directory Project (Segnala (http://www.dmoz.org/public/suggest?cat=Computers/Security/Malicious_Software/) su DMoz un collegamento pertinente all'argomento "Malicious Software")

Pharming

In ambito informatico si definisce **pharming** una tecnica di cracking, utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri *dati sensibili*, come numero di conto corrente, nome utente, *password*, numero di carta di credito etc.

Etimologia

La parola deriva da **farming**, *esternalizzazione*, sul modello di **phishing/fishing**.

Premessa

Ogni volta che un utente digita nel proprio browser l'indirizzo di una pagina web nella forma *alfanumerica* (come www.pincopallino.it) questo viene tradotto automaticamente dai calcolatori in un **indirizzo IP** numerico che serve al protocollo IP per reperire nella rete internet il percorso per raggiungere il server web corrispondente a quel *dominio*. In tal senso, p.es., digitando l'URL *it.wikipedia.org* questo viene tradotto dal Server DNS del proprio provider in un indirizzo IP nel formato 145.97.39.155

L'obiettivo finale del pharming è il medesimo del phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima.

Metodologia di attacco

Esistono almeno due metodologie di attacco, a seconda che l'obiettivo primario sia il Server DNS dell'Internet Service Provider oppure direttamente il PC della vittima:

1. nel primo caso l'utente malintenzionato (cracker) opera, con sofisticate tecniche di intrusione, delle variazioni nei Server DNS dell'Internet Service Provider modificando gli abbinamenti tra il dominio (*es. wikipedia.org*) e l'indirizzo IP corrispondente a quel dominio. In questo modo gli utenti connessi a quel Provider, pur digitando il corretto indirizzo URL, verranno inconsapevolmente reindirizzati ad un server trappola appositamente predisposto per carpire le informazioni. Questo server trappola è ovviamente reperibile all'indirizzo IP inserito dal cracker e l'aspetto del sito è esteticamente simile a quello vero.
2. nel secondo caso l'utente malintenzionato (cracker) opera, con l'ausilio di programmi trojan o tramite altro accesso diretto, una variazione nel personal computer della vittima. Ad esempio, nei sistemi basati sul sistema operativo Windows, modificando il file "hosts" presente nella directory **"C:\windows\system32\drivers\etc"**. Qui possono essere inseriti o modificati gli abbinamenti tra il dominio interessato (*es. wikipedia.org*) e l'indirizzo IP corrispondente a quel dominio. In questo modo la vittima che ha il file **hosts** modificato, pur digitando il corretto indirizzo URL nel proprio browser, verrà reindirizzata verso un server appositamente predisposto per carpire le informazioni. Un altro metodo consiste nel modificare direttamente nel registro di sistema i server DNS predefiniti. In questo modo l'utente - senza rendersene conto - non utilizzerà più i DNS del proprio Internet Service Provider, bensì quelli del cracker, dove ovviamente alcuni abbinamenti fra dominio e indirizzo IP saranno stati alterati.

In tutto questo processo nulla può far ipotizzare alla vittima di essere connessa ad un server trappola se quest'ultimo è perfettamente somigliante a quello vero. Il cracker utilizzerà quindi a proprio beneficio i dati inseriti dalla vittima nel Server "clone".

Come difendersi

Per difendersi dall pharming non esistono alla data di redazione di questo articolo dei programmi **specifici** se non i firewall che tentano di impedire l'accesso al proprio PC da parte di utenti esterni e programmi antivirus che bloccano l'esecuzione di codice malevolo. Per quanto riguarda invece il server DNS dell'Internet Service Provider questo è solitamente gestito e protetto da professionisti che dovrebbero conoscere le modalità di protezione dei propri server.

Se il sito a cui ci si collega è un sito *sicuro* prima dell'accesso verrà mostrato un **certificato digitale** emesso da una **autorità di certificazione** conosciuta, che riporterà i dati esatti del sito. Questo certificato andrebbe quantomeno letto e non frettolosamente accettato. In alcuni casi il sito *sicuro* non appare come tale solo perché la banca utilizza una tecnica di incapsulamento delle pagine a *frames* che non mostra il lucchetto nell'apposita casellina del browser né l'indirizzo in modalità *https*.

Voci correlate

- Spoofing
- Certificato digitale
- Cracker
- Sicurezza informatica
- Hacker
- Firewall
- Antivirus

Phishing

Il **phishing** è un tipo di truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.

Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito. Tale truffa può essere realizzata anche mediante contatti telefonici o con l'invio di SMS (SMISHING)

La prima menzione registrata del termine phishing è sul newsgroup di Usenet *alt.online-service.america-online* il 2 gennaio 1996,[1] malgrado il termine possa essere apparso precedentemente nell'edizione stampata della rivista per hacker *2600*.[2] Il termine phishing è una variante di *fishing* (letteralmente "pescare" in lingua inglese),[3] probabilmente influenzato da *phreaking*[4][5] e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente. La parola può anche essere collegata al linguaggio leet, nel quale la lettera f è comunemente sostituita con ph.[6] La popolare teoria che si tratti di un portmanteau di *password harvesting*[7] è un esempio di pseudoetimologia.

Metodologia di attacco

Il processo standard delle metodologie di attacco di *phishing* può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (*phisher*) spedisce al malcapitato e ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'e-mail contiene quasi sempre avvisi di *particolari situazioni o problemi* verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login).
4. il link fornito, tuttavia, *non* porta in realtà al sito web ufficiale, ma a una *copia fittizia* apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Talora, l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro" (quale operatore finanziario o *financial manager*), consistente nel fornire le coordinate bancarie del proprio conto online per ricevere l'accredito di somme che vanno poi ri-trasferite all'estero tramite sistemi di *money trasfert* (Western Union o Money Gram), trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. In realtà si tratta del denaro rubato con il *phishing*, per il quale il titolare del conto online beneficiario, spesso in buona fede, commette il reato di riciclaggio di denaro sporco. Quest'attività comporta per il *phisher* la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il denaro sottratto in molti conti correnti e a fare ritrasferimenti in differenti Paesi, perché così diviene più difficile risalire alla identità del criminale informatico e ricostruire compiutamente il meccanismo illecito. Peraltro, se i trasferimenti coinvolgono più Paesi, i tempi per la ricostruzione dei movimenti bancari si allungano, poiché spesso serve una rogatoria e l'apertura di un procedimento presso la magistratura locale di ogni Paese interessato.[8]

Difesa

Bisogna fare attenzione ai siti visitati non autentici. In caso di richiesta di dati personali, numeri di conto, password o carta di credito, è buona norma, prima di cancellare, inoltrarne una copia alle autorità competenti e avvisare la banca o gli altri interessati, in modo che possano prendere ulteriori disposizioni contro il sito falso e informare i propri utenti.

Il cliente può verificare i movimenti dall'estratto conto, che può vedere al Bancomat o dal proprio conto corrente on-line.

Molti istituti offrono un servizio di *SMS alert*, più efficace, perché notifica il movimento non appena viene effettuato, non quando avviene la sua registrazione, che può essere a distanza di diversi giorni. Il servizio è attivabile dal Bancomat, in filiale o dall'ambiente on-line, e consiste nell'invio di un messaggio al numero indicato dal cliente, per tutti i prelievi o pagamenti che superano l'importo da questi impostato. Il messaggio parte in tempo reale quando è effettuato il movimento (non alla data di registrazione, quindi anche quando questo non è ancora visibile nell'estratto conto).

Il servizio è gratuito; i costi del messaggio dipendono dall'operatore telefonico. La Banca non è obbligata a fornire questo tipo di servizio, e le compagnie telefoniche non garantiscono il ricevimento degli SMS in tempi certi, che possono aumentare in particolare se il cliente si trova all'estero con il suo terminale di ricezione.

La persona che si accorge di pagamenti effettuati da terzi con la sua carta di credito o Bancomat, deve contattare il numero verde della banca per chiedere il blocco della carta: la chiamata viene registrata e le è assegnato un codice di blocco (che è identificativo e univoco). Occorre poi presentare denuncia alle Forze di Polizia, e recarsi in Agenzia con la copia della denuncia e il codice di blocco. In caso di eventuali addebiti "anomali" successivi, ad esempio perché effettuati dall'estero e registrati o contabilizzati con valuta successiva al blocco e alla denuncia, è necessario recarsi nuovamente a integrare la denuncia e ripresentarne copia in filiale.
L'Agenzia inoltra all'Ufficio Legale della Banca la ricusazione dei pagamenti e la richiesta di rimborso per la liquidazione. L'Ufficio Legale verifica se il cliente era fisicamente impossibilitato ad effettuare i movimenti contabili (prelievi da conto o pagamenti) perché l'estratto conto o la denuncia provano che si trovava in altro luogo; se vi sia dolo colpa o negligenza; applica una franchigia (intorno ai 150 euro) che non viene rimborsata, se il contratto di attivazione della carta prevede una responsabilità che in questi casi resti comunque a carico del cliente.

In presenza di accrediti da parte di sconosciuti, il correntista deve non prelevare la somma e chiedere alla banca lo storno del movimento contabile.

Una preoccupazione frequente degli utenti che subiscono lo spillaggio è capire come ha fatto il perpetratore a sapere che hanno un conto presso la banca o servizio online indicato nel messaggio-esca. Normalmente, il *phisher* non conosce se la sua vittima ha un account presso il servizio preso di mira dalla sua azione: si limita ad inviare lo stesso messaggio-esca a un numero molto elevato di indirizzi di email, facendo spamming, nella speranza di raggiungere per caso qualche utente che ha effettivamente un account presso il servizio citato. Pertanto non è necessaria alcuna azione difensiva a parte il riconoscimento e la cancellazione dell'email che contiene il tentativo di spillaggio.

Nel caso del problema correlato noto come Pharming, invece, non esiste una vera e propria soluzione a posteriori ed è necessaria un'azione preventiva.

Un primo controllo per difendersi dai siti di spillaggio, è quello di visualizzare l'icona, a forma di lucchetto in tutti i *browser*, che segnala che sì è stabilita una connessione sicura (ad esempio una connessione SSL/TLS). Tale connessione garantisce la riservatezza dei dati, mentre la loro integrità e l'autenticazione della controparte avvengono solo in presenza della firma digitale, che è *opzionale* e non segnalata.

Infatti, una connessione SSL potrebbe essere stabilita con certificati non veritieri, tramite una coppia di chiave pubblica e privata valide, note a chi vuole fare *phishing*, ma che non sono quelle effettive del sito. Ad esempio, il certificato riporta che il sito it.wikipedia.org utilizza una chiave pubblica, che in realtà è quella del *phisher*. Il *browser* piuttosto che l'utente interessato dovrebbero collegarsi al sito di una *certification authority* per controllare: la banca dati mostra le chiavi pubbliche e un identificativo del possessore, come l'indirizzo IP o l'indirizzo del sito.

Alcuni siti hanno una barra antiphishing specifica che controlla l'autenticità di ogni pagina scaricata dal sito, ad esempio tramite la firma digitale.

La pagina di *login* di un sito è facilmente imitabile. Nei *browser* esiste una opzione per visualizzare il codice HTML delle pagine Internet, che si può copiare e incollare altrove, per ottenere un sito identico. La e-mail truffaldina conterrà un collegamento che punta non al sito originario, ma alla sua imitazione. I dati inseriti nei campi liberi della *form* sono memorizzati in un database o in un file di testo collegato al sito.

Un'altra tecnica di spillaggio consiste nell'inserimento di applicativi di keylogging. In questo caso, i link possono rimandare al sito originale, non necessariamente a un'imitazione, e lo spillaggio dei dati avviene al momento del loro inserimento da tastiera. Queste righe di codice possono essere eseguite con l'apertura di alcuni link, ovvero con la lettura della stessa e-mail, se il programma di posta o l'Internet Service Provider non adottano protezioni sufficienti.

Esistono, inoltre, programmi specifici come la barra anti-spillaggio di Netcraft e anche liste nere (*blacklist*), che consentono di avvisare l'utente quando visita un sito probabilmente non autentico. Gli utenti di Microsoft Outlook / Outlook Express possono proteggersi anche attraverso il programma gratuito Delphish, un toolbar inserito nel MS Outlook / MS Outlook Express con il quale si può trovare i link sospetti in un'email (vedi sezione Collegamenti esterni). Questi programmi e i più comuni browser non si avvalgono di *whitelist* contenenti gli indirizzi logici e IP

delle pagine di autenticazione di tutti gli istituti di credito, che sarebbe un filtro anti-spillaggio sicuramente utile.

Se l'utente non è titolare di un conto corrente online e riceve gli estratti conto periodici per posta ordinaria (non via email), può impostare il filtro anti-spam, inserendo l'indirizzo dell'istituto di credito. In questo modo, le email contenenti un indirizzo del mittente o un link nel testo alla banca, saranno inserite nella cartella dello *spam*, rendendo più facilmente identificabili quelle sospette.

Gli utenti di Internet Explorer possono utilizzare un filtro anti-spillaggio che utilizza una *blacklist*, e confronta gli indirizzi di una pagina web sospetta con quelli presenti in una banca dati mondiale e centralizzata, gestita da Microsoft e alimentata dalle segnalazioni anonime degli utenti stessi.

Analoga protezione è presente in Mozilla Firefox (a partire dalla versione 2), che propone all'utente di scegliere tra la verifica dei siti sulla base di una *blacklist* e l'utilizzo del servizio anti-spillaggio offerto da Google.

Mancano invece banche dati di questo tipo condivise dai vari produttori di browser, pubbliche o istituite presso autorità che hanno la competenza sulle tematiche di Internet e del web (in Italia, la Polizia Postale).

L'oscuramento di un sito di spillaggio non è un'operazione semplice, se questo è ospitato come sottodominio di un altro indirizzo web. In quel caso, è necessario l'oscuramento del dominio ospitante, poiché la "falsa" pagina di autenticazione non è presente nell'elenco ICANN, ma in locale sul server. Il sito oscurato può essere comunque velocemente associato ad un altro indirizzo web.

È possibile associare ad una pagina di un "sito esca" un indirizzo simile, ma non identico a quello del sito "copiato".

All'utente medio resta comunque difficile distinguere un sito di phishing da quello dell'istituto di credito preso di mira. La barra degli indirizzi può contenere un indirizzo del tipo "Nome della Banca.autethicationPage.php@indirizzo del dominio ospitante", l'indirizzo del dominio ospitante nel corrispondente indirizzo IP, il simbolo "@" nella codifica ASCII, o nell'equivalente binario o esadecimale, rendendo l'indirizzo della risorsa di "phishing" simile e poco più lungo di quello che è stato falsificato.

Risarcimento del danno

Per la normativa italiana, gli istituti di credito non sono tenuti a garantire i clienti da frodi informatiche. Non sono perciò tenute al risarcimento delle somme prelevate indebitamente a causa di una violazione dell'*account* Internet dei clienti, o della clonazione dei loro bancomat o carte di credito.

Un recente provvedimento del GUP di Milano, del 10 ottobre 2008, ha stabilito che solo l'esistenza di un preciso obbligo contrattuale in capo alla banca di tenere indenne il cliente da ogni tipo di aggressione alle somme depositate potrebbe attribuire all'ente la qualifica di danneggiato dal reato.

I singoli contratti per l'apertura di un conto corrente e la *home banking* possono prevedere che in specifici casi la banca sia tenuta a risarcire il cliente delle somme indebitamente prelevate.

Spesso, l'istituto di credito è coperto dal rischio di furto o smarrimento dei dati identificativi e delle carte. Il costo di questa riassicurazione è ribaltato sui clienti, che talora beneficiano di clausole contrattuali a loro favore per questo tipo di coperture.

L'istituto rifiuta generalmente il risarcimento se il cliente, oltre a perdere la carta, ha smarrito anche il PIN di accesso; in modo analogo, per la *home banking* rifiuta di risarcire le somme se il cliente ha smarrito la *password* di accesso insieme al *token*. Ciò configura negligenza da parte del cliente e l'eventualità del dolo e truffa all'istituto di credito: il cliente potrebbe cedere a terzi i propri dati e la carta, i quali, d'accordo col cliente, potrebbero effettuare dei prelievi, mentre il titolare dichiara lo smarrimento o il furto.

Tuttavia la banca (o altro istituto o società) ha l'onere di applicare sia le misure di sicurezza minime stabilite nel DL 196/03 per tutelare i dati personali del cliente, sia di attuare tutte quelle misure idonee e preventive che, anche in base al progresso tecnico, possono ridurre al minimo i rischi. Infatti in caso di furto delle credenziali, anche se la banca accusa l'utente di esserne responsabile perché potrebbe aver risposto a mail di phishing, è tenuta a dimostrare

al giudice di aver attuato tutte le misure (sia quelle minime stabilite che quelle idonee e preventive che vanno valutate di caso in caso con una valutazione del rischio -obbligatoria- e un documento programmatico per la sicurezza) per ridurre al minimo i rischi. Se la banca non ha attuato misure che in altre banche sono comuni per la prevenzioni delle frodi informatiche, accessi abusivi etc., ad esempio, potrebbe essere tenuta a risarcire l'utente del danno.

La Raccomandazione europea n. 489 del 1997 stabilisce che dalla data della comunicazione alla banca di aver subito una truffa (con allegazione della denuncia alla polizia), il titolare del conto non può essere ritenuto responsabile dell'uso che viene fatto del suo conto da parte di terzi, per cui i soldi sottratti devono essergli restituiti.

Casi giudiziari e prime condanne penali

Nel 2007 con sentenza del Tribunale di Milano [9] si è avuta, per la prima volta in Italia, la condanna di membri di una associazione transnazionale dedita alla commissione di reati di *phishing* [10]. Tale sentenza è stata confermata in Cassazione nel 2011.

Nel 2008, con sentenza del Tribunale di Milano [11], si è invece pervenuti per la prima volta in Italia alla condanna per riciclaggio [12] di soggetti che, quali *financial manager*, si erano prestati alla attività di incasso e ritrasferimento di somme di denaro provento dei reati di *phishing* a danno dei correntisti italiani [13]

Queste due sentenze hanno dunque indicato quali norme possono essere applicate a questo nuovo fenomeno criminale, dal momento che in Italia il *phishing* non è ancora specificatamente regolamentato, a differenza di altre legislazioni - prima fra tutte quella americana - che possiedono norme penali incriminatrici *ad hoc* [14]

Note

[1] *"phish, v." OED Online, March 2006, Oxford University Press.* (http://dictionary.oed.com/cgi/entry/30004303/) in *Oxford English Dictionary Online*. URL consultato in data 9 agosto 2006.

[2] Ollmann, Gunter. *The Phishing Guide: Understanding and Preventing Phishing Attacks* (http://www.technicalinfo.net/papers/Phishing.html) in *Technical Info*. URL consultato in data 10 luglio 2006.

[3] *Spam Slayer: Do You Speak Spam?* (http://www.pcworld.com/article/id,113431-page,1/article.html) in *PCWorld.com*. URL consultato in data 16 agosto 2006.

[4] *"phishing, n." OED Online, March 2006, Oxford University Press.* (http://dictionary.oed.com/cgi/entry/30004304/) in *Oxford English Dictionary Online*. URL consultato in data 9 agosto 2006.

[5] *Phishing* (http://itre.cis.upenn.edu/~myl/languagelog/archives/001477.html) in *Language Log, 22 settembre 2004*. URL consultato in data 9 agosto 2006.

[6] Anthony Mitchell. *A Leet Primer* (http://www.technewsworld.com/story/47607.html.), TechNewsWorld, 12 luglio 2005.

[7] *Know your Enemy: Phishing* (http://www.honeynet.org/papers/phishing/) in *The Honeynet Project & Research Alliance*. URL consultato in data 8 luglio 2006.

[8] F.Cajani, G. Costabile, G. Mazzaraco, *Phishing e furto d'identita digitale. Indagini informatiche e sicurezza bancaria*, Milano, Giuffrè, 2008

[9] Tribunale di Milano, sentenza del 10.12.2007 - est. Gamacchio (Giudice per l'udienza preliminare): cfr. R. Flor, *Frodi identitiarie e diritto penale*, in *Riv. giurisp. econ. az.*, 2008, 4, p. 184; A. Sorgato, I*l reato informatico: alcuni casi pratici*, in *Giur. pen.*, 2008, 11, p. 40

[10] L. Fazzo, «Ecco come noi hacker romeni vi svuotiamo i conti bancari» (http://www.ilgiornale.it/interni/ecco_come_noi_hacker_romeni_vi_svuotiamo_conti_bancari/11-12-2007/articolo-id=226695-page=0-comments=1), in *Il Giornale*, 11 dicembre 2007

[11] Tribunale di Milano, sentenza del 29.10.2008, est. Luerti (Giudice per l'udienza preliminare) in *Corr. Mer.*, 2009, 3, pp. 285 e ss. con nota di F. Agnino, *Computer crime e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*

[12] L. Ferrarella , Soldi trasferiti online. «È riciclaggio» (http://archiviostorico.corriere.it/2009/gennaio/07/Soldi_trasferiti_online_riciclaggio__co_7_090107025.shtml), in *Corriere della Sera*, 7 gennaio 2009

[13] F. Tedeschi, Lotta al cybercrime. Intervista esclusiva al magistrato a caccia delle nuove mafie (http://www.osservatoriofinanziario.it/of/newslarge.asp?id=636&pagina=1)

[14] S. Aterno, F. Cajani, G. Costabile, M. Mattiucci, G. Mazzaraco, *Computer Forensics e indagini digitali*, Experta, 2011

Voci correlate

- Truffa alla nigeriana
- Scam
- Skimmer
- Pharming
- Vishing
- Trashing
- Whaling
- Tabnabbing
- Keylogger
- Script kiddie
- Cracker
- Cracking
- Ingegneria sociale
- Social Network Poisoning

Collegamenti esterni

- HOAX.IT - Tutto su Bufale, Leggende Metropolitane, Verifica Hoax e Appelli Umanitari, Sicurezza Informatica, Phishing, Truffe, News (http://www.hoax.it/)
- Phishing (en) (http://www.dmoz.org/Society/Crime/Theft/Identity_Theft/Phishing/) su Open Directory Project (Segnala (http://www.dmoz.org/public/suggest?cat=Society/Crime/Theft/Identity_Theft/Phishing/) su DMoz un collegamento pertinente all'argomento "Phishing (en)")
- Anti-Phishing Italia (http://www.anti-phishing.it/)
- SicurezzaInformatica.it - Categoria Phishing e Truffe (http://www.sicurezzainformatica.it/archives/phishing_e_truffe/)
- Truffe on-line: news ed informazioni sulle frodi, trappole, inganni, raggiri ed insidie perpetrate in Rete e nel mondo reale (http://www.truffeonline.it/)
- (**EN**) Anti-Phishing Working Group (http://www.antiphishing.org/)
- (**EN**) Anti-phishing Toolbars (http://www.xml-dev.com/blog/index.php?action=viewtopic&id=59) Free Anti-phishing Toolbars for Web Browsers.
- (**EN**, **DE**) Delphish (http://www.delphish.com) Free Anti-phishing-Tool for MS Outlook
- (**EN**) Safe Browsing for Enterprise Users (http://www.xml-dev.com/xml/SafeBrowsing/) How Enterprises can make web browsing safer by using free software applications.
- dirittodellinformatica.it (http://www.dirittodellinformatica.it/focus/privacy-e-sicurezza.html) Segnalazioni di casi di phishing
- diritto penale e diritto penale dell'informatica Riferimenti bibliografici e articoli sui profili penali del phishing (http://www.robertoflor.blogspot.com/)
- Prevenzione Svizzera della Criminalità - Phishing (http://www.conosco-il-trucco.ch/4/it/1metodi_di_prevenzione_e_truffa/40206phishing.php)
- Procura della Repubblica presso il Tribunale di Milano - pool reati informatici (http://www.procura.milano.giustizia.it/reati-informatici.html)

Script kiddie

Script kiddie è un termine dispregiativo utilizzato per indicare quegli individui che utilizzano istruzioni, codici e programmi ideati da altri, al massimo con leggere modifiche, facendo intendere di essere un grande *guru* dell'informatica. Il termine script kiddie è stato coniato dagli hacker, verso la fine degli anni 1990, quando la diffusione dei sistemi operativi open source e degli accessi privati a internet cominciavano ad allargare il pubblico di persone interessate al funzionamento dei personal computer, con il conseguente aumento di persone con pochi scrupoli e imitatori in cerca di notorietà.

Chi è lo script kiddie

Lo script kiddie è qualcuno alla ricerca di una intrusione facile. Il loro obiettivo è quello di ottenere i privilegi di root nel modo più semplice possibile. Per ottenere ciò si concentrano su un piccolo numero di vulnerabilità, cercandole su tutta la rete. Alcuni di loro non hanno idea di quello che stanno facendo. Comunque, a prescindere dal loro livello di preparazione, hanno una strategia comune: cercare in modo casuale vulnerabilità specifiche e sfruttare queste debolezze. Sono persone incapaci di produrre autonomamente gli strumenti adatti alle proprie attività e di capire pienamente il funzionamento di quelli che utilizzano. Si definisce tale, il ragazzino che utilizzando strumenti e software comuni nell'ambiente dell'underground attacca sistemi remoti in modo sistematico. La loro competenza è leggermente al di sopra di quella dell'utente medio. Spesso chi svolge tale attività non ha nemmeno idea di cosa stia facendo, e sicuramente non è cosciente delle conseguenze delle sue azioni. Non è il genere di hacker che esplora, ma piuttosto che utilizza quanto è già disponibile. Gli script kiddie sono la forma meno evoluta di cracker. Sono persone che non sanno programmare, ma che creano pagine HTML scadenti copiando funzioni di JavaScript da altre pagine HTML scarse. Più genericamente, uno script kiddie scrive (o più precisamente copia e incolla) un codice senza avere o desiderare di avere un'idea di quello che il codice faccia. Una variante di script kiddie è il lamer.

Le metodologie

La metodologia usata è semplice. Gli script kiddie esplorano Internet per una specifica vulnerabilità, e quando la trovano, la sfruttano. Molti degli strumenti usati sono automatici e richiedono solo una piccola interazione. Lanciano lo strumento e poi tornano a controllare il risultato qualche giorno dopo. Non ci sono due script uguali così come non ci sono vulnerabilità uguali. Comunque molti di questi strumenti usano la stessa strategia. Per prima cosa costruiscono un archivio di indirizzi IP. Quindi li testano per una specifica vulnerabilità. Inoltre i risultati di queste operazioni sono spesso archiviati o condivisi tra diversi utenti per essere usati in un altro momento. In definitiva uno script kiddie può attaccare con successo il vostro sistema senza averlo mai esaminato prima.

Gli aggressori più smaliziati, una volta compromesso il sistema piazzano trojans e backdoor. Le backdoor (porte di servizio) permettono un facile e sicuro accesso al sistema in qualsiasi momento. I trojans (cavalli di troia) rendono invisibile l'intruso. Egli non sarà visibile in nessun log, processo di sistema o struttura file. Avrà un posto sicuro da dove potrà continuare a esaminare la Rete. Gli script sono spesso automatici per entrare nel sistema, esistono strumenti automatici per nascondere le tracce dell'intrusione, spesso chiamati rootkit. Uno dei più comuni rootkit è lrk4. Gli script kiddie attaccano in ogni momento. Lavorano 24 ore al giorno. Inoltre questi attacchi sono lanciati da ovunque nel mondo.

Gli strumenti

Gli strumenti degli script kiddie sono: trojan, zombie, script già pronti, rootkit. Gli strumenti implicati sono estremamente semplici da usare. Molti sono limitati a un singolo fine con poche opzioni. Per primi vengono gli strumenti usati per costruire un database di indirizzi IP. Questi strumenti sono realmente casuali, in quanto esaminano indiscriminatamente Internet. Lo strumento quindi seleziona casualmente quali rete IP esaminare. Un altro strumento usa un nome di dominio. Costruisce un database di indirizzi IP effettuando un trasferimento di zona del nome di dominio e di tutti i sotto domini. Alcuni utenti hanno costruito database con oltre 2 milioni di indirizzi IP esaminando gli interi domini .com e .edu. Una volta scoperti, gli IP vengono esaminati con strumenti atti a determinare varie vulnerabilità, come la versione di named, il sistema operativo, o i servizi in esecuzione sul sistema. Una volta identificato il sistema vulnerabile, l'aggressore colpisce. Le due categorie di strumenti di esplorazione sono: sscan e nmap. Sscan rappresenta lo strumento di esplorazione "tuttofare" dello script kiddie. Esso fa un test della rete per un gruppo di vulnerabilità specifiche. È configurabile, permettendo l'aggiunta di nuovi test di vulnerabilità. L'utente per usarlo deve essere root. Il risultato è un elenco di molti servizi vulnerabili. Nmap rappresenta il gruppo di strumenti "raw data". Non dice quali vulnerabilità esistono, piuttosto dice quali porte sono aperte, cosicché l'utente può determinare l'impatto di sicurezza. A ogni modo è necessario avere conoscenze di rete per usarlo e interpretare i dati.

La minaccia

È la sezione casuale dei bersagli che rende così pericoloso lo script kiddie. I sistemi che gli script kiddie cercano sono i sistemi non protetti che sono facilmente sfruttabili, l'intrusione facile. Tradizionalmente lo script kiddie (letteralmente ragazzino da script) non ha le capacità tecniche di un cracker esperto, ma può essere ugualmente pericoloso per il carattere sistematico su larga scala dei suoi "scan" automatizzati. Gli attacchi degli script kiddie sono innocui per sistemi correttamente configurati e gestiti, in cui sono state applicate le ultime patch di sicurezza. L'80% del traffico maligno su Internet è generato da script kiddie.

Come proteggersi contro questa minaccia

Lo script kiddie è alla ricerca di un'intrusione facile, cerca delle vulnerabilità comuni. Bisogna assicurarsi che i sistemi e le reti non siano soggetti a tali vulnerabilità. Sia www.cert.org [1] sia www.ciac.org [2] sono eccellenti fonti riguardo alle vulnerabilità più comuni. Inoltre, la lista bugtraq (tenuta a securityfocus.com) è una delle migliori fonti di informazione. Un altro modo di proteggersi è quello di eseguire solo i servizi che sono necessari. Se un servizio non è necessario si può eliminarlo. Se un servizio è necessario, assicurarsi di usare l'ultima versione. Per esempi di come fare ciò, leggete Proteggere Solaris, Proteggere Linux o Proteggere NT. I server DNS sono spesso usati per sviluppare database di sistemi che possono essere esaminati. Limitare i sistemi che possono fare trasferimenti di zona a partire dai Name Server. Registrare ogni trasferimento di zona non autorizzato e seguirlo. Controllare se i sistemi sono sotto esame. Una volta identificati, si possono tracciare questi eventi per ottenere una migliore comprensione della minaccia e poter reagire.

Esempi famosi

Gli esempi più famosi di script kiddie includono:

- Uno script kiddie di 15 anni chiamato Mafiaboy è stato arrestato in un quartiere borghese a Montreal nel 2000. Utilizzando strumenti scaricati atti a provocare attacchi DoS (Denial of service), ha inflitto danni a siti web famosi come Yahoo!, Valletta Construction Inc, Amazon.com, eBay e CNN, causando pressappoco 1,7 miliardi di dollari di danno. È stato condannato per 55 reati criminali e ha scontato 8 mesi in un centro di detenzione giovanile e un anno in libertà vigilata.

- Jeffrey Pastore di Riparo, uno studente di scuola superiore di 18 anni del Minnesota responsabile per l'utilizzo della Variante B del virus chiamato Blaster. Il programma ha fatto parte di un attacco DoS contro computer che utilizzano il sistema operativo Microsoft Windows. L'attacco ha preso la forma di un SYN flood che ha solo causato danni marginali. È stato condannato a 18 mesi da scontare in prigione nel 2005.

Voci correlate

- Code monkey
- Lamer
- Hacker
- Cracker
- Sicurezza informatica

Note

[1] http://www.cert.org
[2] http://www.ciac.org

Sicurezza informatica

Con il termine **sicurezza informatica** si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente. Tale protezione è ottenuta attraverso misure di carattere organizzativo e tecnologico tese ad assicurarne l'accesso solo ad utenti autorizzati (autenticazione), la fruizione (disponibilità) di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema, l'oscuramento (cifratura) e la correttezza (integrità) dei dati scambiati in una comunicazione nonché la protezione del sistema da attacchi di software malevoli.

Navy Cyber Defense Operations Command, unità che controlla le attività non autorizzate nei sistemi informativi della United States Navy

Generalità

La sicurezza informatica è un problema sempre più sentito in ambito tecnico-informatico per via della sempre più spinta *informatizzazione* della società e dei servizi (pubblici e privati) in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione degli attaccanti o *hacker*.

L'interesse per la sicurezza dei sistemi informatici è dunque cresciuto negli ultimi anni proporzionalmente alla loro diffusione ed al loro ruolo occupato nella collettività. Molti ex-hacker/cracker sono oggi dirigenti di società di sicurezza informatica o responsabili di questa in grandi multinazionali. Ciò sembra mostrare che per capire le strategie migliori di sicurezza informatica è necessario entrare nella mentalità dell'attaccante per poterne prevedere ed ostacolare le mosse.

Il raggiungimento della disponibilità dipende da diversi fattori che interferiscono tra utente e sistema, quali: robustezza del software di base e applicativo, affidabilità delle apparecchiature e degli ambienti in cui essi sono collocati.

Il sistema informatico deve essere in grado di impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia da eventi accidentali; inoltre deve impedire l'accesso abusivo ai dati.

“In generale non è buona norma assumere che le contromisure adottate in un sistema siano sufficienti a scongiurare qualsiasi attacco".

Parametri di protezione

I principali aspetti di protezione del dato sono la confidenzialità (o riservatezza), l'integrità dei dati e la disponibilità.

La protezione dagli attacchi informatici viene ottenuta agendo su più livelli: innanzitutto a livello fisico e materiale, ponendo i server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi; anche se questo accorgimento fa parte della sicurezza normale e non della "sicurezza informatica" è sempre il caso di far notare come spesso il fatto di adottare le tecniche più sofisticate generi un falso senso di sicurezza che può portare a trascurare quelle semplici. Il secondo livello è normalmente quello logico che prevede l'autenticazione e l'autorizzazione di un'entità che rappresenta l'utente nel sistema. Successivamente al processo di autenticazione, le operazioni effettuate dall'utente sono tracciate in file di log. Questo processo di monitoraggio delle attività è detto audit o accountability.

Per evitare invece gli eventi accidentali, non esistono soluzioni generali, ma di solito è buon senso dell'utente fare una copia di backup del sistema, fare backup periodico di dati e applicazioni in modo da poter fronteggiare qualsiasi danno imprevisto.

Analisi del rischio

Tipicamente questa precede la fase di messa in sicurezza del sistema informatico la cosiddetta analisi del rischio ovvero la valutazione di tutte le possibili minacce in termini di probabilità di occorrenza e relativo danno potendo così stimare il relativo rischio: in base a tale valore si decide se, come e quali contromisure di sicurezza adottare.

Principali cause di perdita di dati

Le cause di probabile perdita di dati nei sistemi informatici possono essere molteplici, ma in genere vengono raggruppate in due eventi:

- Eventi indesiderati;
- Eventi accidentali.

Eventi indesiderati

Tra i due eventi sopra citati, quelli indesiderati sono quelli per lo più inaspettati, anche se è prudente aspettarsi di tutto, e sono i cosiddetti attacchi da parte di utenti non autorizzati al trattamento di dati o all'utilizzo di servizi. Alcuni degli eventi indesiderati che si possono subire possono essere:

- Attacchi hacking;
- Uso delle proprie autorizzazioni per l'accesso a sistemi da parte di utenti non autorizzati.

Attacchi hacking

Gli attacchi hacking, spesso conosciuti sotto il nome di attacchi cracker, vengono fatti tramite la rete internet, da parte di utenti chiamati appunto dalla società "cracker", che tramite l'uso di software particolari, a volte creati da loro stessi, si intrufolano abusivamente all'interno del sistema, riuscendo ad ottenere piena disponibilità della macchina, per gestire risorse e dati senza avere i giusti requisiti richiesti.

Accesso a sistemi da parte di utenti non autorizzati

Questo tipo di attacco sostanzialmente è simile al precedente, ma ha una forma diversa. Questo attacco consiste nell'uso non autorizzato di sistemi e di dati altrui, ma a differenza di un attacco cracker stavolta viene usata la macchina e non la rete.

Effetti

La pericolosità degli attacchi in quanto tale, consiste non solo nella presa di possesso di requisiti, dati e servizi altrui, ma anche causa all'utente cosiddetto "derubato" una sorta di insicurezza a far fede sui sistemi informatici che spesso fanno parte della nostra vita quotidiana.

Eventi accidentali

Gli eventi accidentali non fanno riferimento ad un attacco da parte di terzi, ma fanno riferimento a eventi causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, incompatibilità di parti hardware, guasti imprevisti, ecc… Tutti eventi che comunque compromettono la sicurezza del sistema soprattutto in termini di disponibilità. Per far fronte a tali evenienze molte volte si opera in un contesto di ridondanza degli apparati (es. server cluster) ovvero con sistemi distribuiti all'interno di piani di disaster recovery che, assicurando la tolleranza ai guasti (fault tolerance), garantiscano affidabilità e disponibilità cioè il business continuity del sistema informatico e dell'azienda.

Tipi di sicurezza e di attacchi

Proprio sulla base di queste osservazioni, quando si parla di "sicurezza informatica" spesso si distinguono i concetti di *sicurezza passiva* e di *sicurezza attiva*.

Sicurezza passiva

Per *sicurezza passiva* normalmente si intendono le tecniche e gli strumenti di tipo *difensivo*, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata. Il concetto di sicurezza passiva pertanto è molto generale: ad esempio, per l'accesso a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.

Sicurezza attiva

Per *sicurezza attiva* si intendono, invece, tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non autorizzato possa modificarli (integrità).

È evidente che la sicurezza passiva e quella attiva siano tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.

Le possibili tecniche di attacco sono molteplici, perciò è necessario usare contemporaneamente diverse tecniche difensive per proteggere un sistema informatico, realizzando più barriere fra l'attaccante e l'obiettivo.

Spesso l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, quanto piuttosto dai dati in essi contenuti, quindi la sicurezza informatica deve preoccuparsi di impedire l'accesso ad utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a certe operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati.

Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc. La sicurezza informatica si occupa anche di prevenire eventuali situazioni di Denial of service (DoS). I DoS sono attacchi sferrati al sistema con l'obiettivo di renderne inutilizzabili alcune risorse in modo da danneggiare gli utenti del sistema. Per prevenire le violazioni si utilizzano strumenti hardware e software.

Sicurezza nelle aziende

Dal momento che l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. Per questo esistono, a carico delle imprese, precisi obblighi in materia di privacy, tra cui quello di redigere annualmente uno specifico documento programmatico sulla sicurezza. È stato anche approvato a livello internazionale il nuovo Standard ISO 27001:2005 finalizzato alla standardizzazione delle modalità adatte a proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità. Lo standard indica i requisiti di un adeguato sistema di gestione della sicurezza delle informazioni (ISMS) finalizzato ad una corretta gestione dei dati dell'azienda. Una fase indispensabile di ogni pianificazione della sicurezza è la valutazione del rischio e la gestione del rischio. Il CLUSIT è l'associazione nazionale che promuove la conoscenza nelle aziende.

Sicurezza dei programmi

Il problema della sicurezza dei programmi e soprattutto dell'invio e ricezione di dati confidenziali protetti, si è posto all'attenzione degli sviluppatori di software come conseguenza della sensibile crescita dell'uso degli strumenti informatici e di internet. Per quanto riguarda la produzione di software "protetti" possiamo partire col definire il concetto di **sicurezza** come **l'assenza da condizioni conflittuali capaci di produrre danni mortali o irreparabili ad un sistema.** Nella progettazione di software è quindi fondamentale raggiungere il compromesso più funzionale tra l'efficienza d'uso del programma in questione e la sua capacità di "sopravvivenza" ad attacchi esterni e ad errori più o meno critici.

Caratteristiche di sicurezza

Due caratteristiche fondamentali esplicano il concetto di sicurezza:

- **Safety** (sicurezza): una serie di accorgimenti atti ad eliminare la produzione di danni irreparabili all'interno del sistema;
- **Reliability** (affidabilità): prevenzione da eventi che possono produrre danni di qualsiasi gravità al sistema.

Un software (o programma) è tanto più sicuro quanto minori sono le probabilità che si verifichi un guasto e la gravità del danno conseguente al guasto stesso. Possiamo ora vedere, in ordine crescente, i possibili effetti dei guasti in cui può incorrere un software:

- Nessun effetto
- Rischio trascurabile
- Rischio significativo
- Rischio elevato
- Rischio catastrofico.

Controllo della sicurezza di un programma

Una volta prodotto il software si procede alla verifica del suo comportamento, in modo tale da effettuare una ricerca estesa dei difetti presenti, per passare poi alla loro eventuale eliminazione. Esistono diversi modelli di sicurezza per il controllo dei programmi basati su due metodi differenti:

- **Semantic-based security model** (modelli di sicurezza basati sulla semantica): la sicurezza del programma controllato viene esaminata in termini di comportamento del programma
- **Security-typed language** (modelli di sicurezza basati sul linguaggio): i tipi delle variabili sono seguiti dall'esplicazione delle politiche adottate per l'uso dei dati battuti.

Per essere efficace un programma deve essere controllato nelle sue specifiche e deve essere privo di difetti nel codice, a questo fine viene effettuato un controllo delle specifiche del programma e delle prestazioni correlate all'affidabilità, in secondo luogo viene analizzata ogni parte di codice e funzione del sistema.

Errori di programma

L'IEEE (**Institute of Electrical and Electronics Engineers**) ha catalogato gli errori nel software in tre diverse voci a seconda della natura degli errori stessi. Esse sono:

- **Error**: è un errore umano verificatosi durante il processo di interpretazione delle specifiche oppure durante l'uso di un metodo o nel tentativo di risoluzione di un problema
- **Failure**: è un comportamento del software imprevisto ed incongruo rispetto alle specifiche del programma stesso
- **Fault**: è un difetto del codice sorgente.

Gli **errori di programma non nocivi**, come ad esempio gli spyware ed il buffer overflow hanno la caratteristica di non modificare i file di sistema e non recare danno alle caratteristiche del sistema stesso. Troviamo qui sotto elencati una serie di errori e di attacchi al software di differente entità.

Principali tecniche di attacco

- Exploit
- Buffer overflow
- Shellcode
- Cracking
- Backdoor
- Port scanning
- Sniffing
- Keylogging
- Spoofing
- Trojan
- Virus informatici
- DoS
- Ingegneria sociale
- Social Network Poisoning
- CMD Tramite Browser

Principali tecniche di difesa

- Antivirus: consente di proteggere il proprio personal computer da software dannosi conosciuti come virus. Un buon antivirus deve essere costantemente aggiornato ad avere in continua esecuzione le funzioni di scansione in tempo reale. Per un miglior utilizzo l'utente deve avviare con regolarità la scansione dei dispositivi del PC (dischi fissi, CD, DVD e dischetti floppy), per verificare la presenza di virus, worm. Per evitare la diffusione di virus è inoltre utile controllare tutti i file che si ricevono o che vengono spediti tramite posta elettronica facendoli verificare dall'antivirus correttamente configurato a tale scopo.
- Antispyware: software facilmente reperibile sul web in versione freeware, shareware o a pagamento. È diventato un utilissimo tool per la rimozione di "file spia", gli spyware appunto, in grado di carpire informazioni riguardanti le attività on line dell'utente ed inviarle ad un'organizzazione che le utilizzerà per trarne profitto.
- Firewall: installato e ben configurato un firewall garantisce un sistema di controllo degli accessi verificando tutto il traffico che lo attraversa. Protegge contro aggressioni provenienti dall'esterno e blocca eventuali programmi presenti sul computer che tentano di accedere ad internet senza il controllo dell'utente.
- Firma digitale, Crittografia: è possibile proteggere documenti e dati sensibili da accessi non autorizzati utilizzando meccanismi di sicurezza specifici quali: la crittografia, la firma digitale, e l'utilizzo di certificati digitali e algoritmi crittografici per identificare l'autorità di certificazione, un sito, un soggetto o un software.
- Backup: più che un sistema di difesa si tratta di un utile sistema per recuperare dati eventualmente persi o danneggiati. Il backup consiste nell'esecuzione di una copia di sicurezza dei dati di un personal computer o comunque di dati considerati importanti onde evitare che vadano perduti o diventino illeggibili.
- Honeypot: un honeypot (letteralmente: "barattolo del miele") è un sistema o componente hardware o software usato come "trappola" o "esca" a fini di protezione contro gli attacchi di pirati informatici. Solitamente consiste in un computer o un sito che sembra essere parte della rete e contenere informazioni preziose, ma che in realtà è ben isolato e non ha contenuti sensibili o critici; potrebbe anche essere un file, un record, o un indirizzo IP non utilizzato.
- Intrusion Detection System (IDS): è un dispositivo software e hardware (a volte la combinazione di tutti e due) utilizzato per identificare accessi non autorizzati ai computer. Le intrusioni rilevate possono essere quelle prodotte da cracker esperti, da tool automatici o da utenti inesperti che utilizzano programmi semiautomatici. Gli IDS vengono utilizzati per rilevare tutti gli attacchi alle reti informatiche e ai computer. Un IDS è composto da quattro componenti. Uno o più sensori utilizzati per ricevere le informazioni dalla rete o dai computer. Una console utilizzata per monitorare lo stato della rete e dei computer e un motore che analizza i dati prelevati dai sensori e provvede a individuare eventuali falle nella sicurezza informatica. Il motore di analisi si appoggia ad un database ove sono memorizzate una serie di regole utilizzate per identificare violazioni della sicurezza.
- Network Intrusion Detection System (NIDS): sono degli strumenti informatici, software o hardware, dediti ad analizzare il traffico di uno o più segmenti di una LAN al fine di individuare anomalie nei flussi o probabili intrusioni informatiche. I più comuni NIDS sono composti da una o più sonde dislocate sulla rete, che comunicano con un server centralizzato, che in genere si appoggia ad un Database. Fra le attività anomale che possono presentarsi e venire rilevate da un NIDS vi sono: accessi non autorizzati, propagazione di software malevolo, acquisizione abusiva di privilegi appartenenti a soggetti autorizzati, intercettazione del traffico (sniffing), negazioni di servizio (DoS).
- Steganografia: La steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli, mentre per la crittografia è non rendere accessibili i dati nascosti a chi non conosce la chiave. La crittanalisi è l'attacco alla crittografia, che mira ad estrarre i dati cifrati senza chiave. L'obiettivo della steganalisi non è quindi quello di estrarre i dati nascosti, ma semplicemente di dimostrarne l'esistenza.
- Sistema di autenticazione: potrebbe rivelarsi utile, in particolare nelle aziende, l'utilizzo di software per l'autenticazione sicura con un secondo elemento di autenticazione basato su un insieme di caratteri disposti in uno schema suddiviso in file e colonne conosciute dall'utente che dovrà poi inserirle in una combinazione di valori per dimostrare di essere in possesso dei dati corretti. Altro sistema, più sofisticato, è quello del riconoscimento

dell'utente tramite l'utilizzo dell'impronta digitale come forma di autenticazione.

Sicurezza della comunicazione

Un altro filone della sicurezza informatica si occupa delle problematiche di sicurezza connesse alla trasmissione di informazioni confidenziali in rete o su qualunque sistema di telecomunicazioni ovvero protezione dei dati in transito e sugli accessi non autorizzati alla varie risorse e servizi di rete. In tale ambito sono diffuse tecniche di crittografia e autenticazione.

Sicurezza della rete Internet

Con la crescita a dismisura di internet e del "www", le problematiche di sicurezza si sono estese anche ad essa e servono quindi idee e principi su cui basarsi. Per far fronte ai rischi che si corrono utilizzandola, l'Unione Europea mette il suo contributo tramite il programma di protezione "Safer Internet".

Sul fronte tecnico le misure di protezione in rete si concretizzano nell'uso di opportuni protocolli di rete quale HTTPS, SSL, TLS, IPsec e SSH che non fanno altro che applicare i metodi crittografici su uno o più livelli di architettura di rete del modello ISO-OSI.

Safer Internet

L'idea del programma di protezione della rete "Safer Internet", è nata a seguito della crescita di internet e per la crescente presenza di bambini a contatto con questo mondo. "Safer Internet" introdotto dal Parlamento Europeo l'11 maggio 2005, vuole promuovere l'uso sicuro di internet soprattutto per i bambini: una rete europea di 21 linee nazionali attraverso le quali gli utenti finali possono denunciare anonimamente la presenza di contenuti illegali su internet, e la creazione di 23 nodi nazionali di sensibilizzazione per promuovere un uso sicuro di internet, rivolto ai bambini, ai genitori e agli insegnanti. Oltre ai provvedimenti di autoregolamentazione e allo sviluppo di tecnologie adeguate, l'istruzione gioca un ruolo chiave. È indispensabile, infatti, la partecipazione e l'istruzione di genitori e insegnanti, troppo spesso digiuni in materia di internet, che seguano con costanza i ragazzi nella navigazione, fornendo loro gli strumenti critici necessari per un approccio consapevole alla rete.

Apparati di sicurezza di rete

Una rete locale può aumentare il suo grado di sicurezza da e verso l'esterno (Internet) attraverso l'uso di sistemi come:

- Firewall;
- Intrusion detection system (IDS);
- Intrusion prevention system (IPS).

Certificazione

Prodotti software o sistemi informatici possono essere certificati nei loro attributi di sicurezza, con valore aggiunto sul prodotto o sistema stesso in termini pubblicitari di sicurezza (certificazione di qualità in termini di sicurezza), da organismi competenti riconosciuti. Tipicamente il processo di certificazione passa attraverso una fase di valutazione del prodotto/sistema (OdV oggetto della valutazione) da parte di un laboratorio di valutazione accreditato, per il quale il committente/sviluppatore dell'operazione ha identificato un cosiddetto *traguardo di sicurezza* (TdS) in termini di specifiche che il suo prodotto dovrebbe assicurare. Compito del valutatore è verificare a mezzo dell'attività valutativa la congruenza o meno del prodotto/sistema alle specifiche di sicurezza richieste dal committente/sviluppatore, attraverso opportuni criteri di valutazione, redigendo poi un rapporto ed un certificato finale di pubblico dominio.

Questioni giuridiche e regolamentazione globale

Una delle principali battaglie e delle lamentele dell'industria degli AntiVirus è quella relativa alla creazione di una regolamentezione unificata e globale, una base di regole comuni per giudicare legalmente, ed eventualmente punire, i crimini informatici e i criminali informatici. Infatti, ancora oggi, anche se una società produttrice di AntiVirus dovesse riuscire a scoprire chi è il criminale informatico dietro alla creazione di un particolare virus o di un malware o di un qualsiasi attacco informatico, spesso le autorità locali non possono comunque agire.[1][2] Questo è principalmente dovuto al fatto che praticamente ogni stato ha una sua propria regolamentazione, differente da quella degli altri stati.

"[Computer viruses] switch from one country to another, from one jurisdiction to another — moving around the world, using the fact that we don't have the capability to globally police operations like this. So the Internet is as if someone [had] given free plane tickets to all the online criminals of the world."[3] (Mikko Hyppönen)

Ed è anche grazie ad alcune società europee produttrici di AntiVirus (e.g. Avira, BullGuard, F-Secure, Frisk, Panda, TG Soft, ...) che, per risolvere il problema, la Commissione Europea ha deciso di fondare l'EC3 (European Cybercrime Centre).[4] L'EC3 è stato ufficialmente aperto il primo gennaio 2013. L'EC3 si focalizzerà nella lotta della UE contro i crimini informatici.[5]

Note

[1] Mikko Hypponen: Fighting viruses, defending the net (http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html)
[2] Mikko Hypponen - Behind Enemy Lines (http://www.youtube.com/watch?v=0TMFRO66Wv4)
[3] Mikko Hypponen: Fighting viruses, defending the net (http://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net.html)
[4] European Cybercrime Centre set for launch (http://www.virusbtn.com/news/2013/01_09.xml?rss)
[5] Europol European Cybercrime Centre (EC3) (https://www.europol.europa.eu/ec3)

Bibliografia

- G. M. Schneider, J. L. Gersting, Informatica, edizione italiana, Apogeo (2007)

Voci correlate

- Security manager
- Crittografia
- ENISA
- Standard di sicurezza informatica
- Standard ISO/IEC 15408:2005
- Standard ISO 27001:2005
- Standard NIST 800-53
- Protezione
- Danneggiamento informatico
- Accesso abusivo ad un sistema informatico o telematico
- Chiave biometrica
- Architettura di reti sicure
- Sicurezza nella telefonia mobile
- Vulnerability Assessment and Mitigation
- Security Operation Center
- Privilege escalation
- Protezione del database

- Data loss prevention
- EBIOS

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Computer security

Collegamenti esterni

- Sicurezza informatica (http://search.dmoz.org/cgi-bin/search?search=Sicurezza+informatica&all=yes&cs=UTF-8&cat=World/Italiano) su Open Directory Project (Segnala (http://www.dmoz.org/public/suggest?cat=) su DMoz un collegamento pertinente all'argomento "Sicurezza informatica")
- Sicurezza informatica Tecniche di attacco e difesa (http://www.notrace.it/)
- L'unità di prevenzione e gestione degli incidenti informatici governativa (CERT-SPC) a tutela della sicurezza informatica del Sistema Pubblico di Connettività (SPC) (http://www.cert-spc.it/)
- Definizione tratta da One Minute Dictionary (http://tv.bitmat.it/view/576/578/0000000198/Cybercrime.html), dizionario in video di BitMAT
- Stefano Mele, Apr 2012, CYBERWEAPONS: Aspetti Giuridici e Strategici (http://www.stefanomele.it/publications/dettaglio.asp?id=298)
- (EN) http://ec.europa.eu/information_society/activities/sip/index_en.htm Safer Internet Europa

Sniffing

Si definisce **sniffing** (dall'inglese, *odorare*), in informatica e nelle telecomunicazioni, l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso.

Gli sniffer intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo. Inoltre possono offrire strumenti di analisi che analizzano ad esempio tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo di rete o per ricostruire lo scambio di dati tra le applicazioni.

Sniffing del traffico locale

Il traffico può essere intercettato da uno degli host coinvolti nella comunicazione, indipendentemente dal tipo di interfaccia di rete su cui viene inviato.

Sniffing in reti locali

Per intercettare i dati in una rete locale è necessario possedere od ottenere l'accesso fisico al mezzo trasmissivo.

Sniffing in reti ethernet non-switched

In questo tipo di reti ethernet il mezzo trasmissivo (cavo coassiale o, attualmente, cavo UTP o STP connesso ad un hub) è condiviso, quindi tutte le schede di rete dei computer nella rete locale ricevono tutti i pacchetti, anche quelli destinati ad altri, selezionando i propri a seconda dell'indirizzo MAC (indirizzo hardware univoco della scheda di rete).

Lo sniffing in questo caso consiste nell'impostare sull'interfaccia di rete la cosiddetta *modalità promiscua*, che disattivando questo "filtro hardware" permette al sistema l'ascolto di tutto il traffico passante sul cavo.

Sniffing in reti ethernet switched

In questo caso l'apparato centrale della rete, definito switch, si occupa di inoltrare su ciascuna porta solo il traffico destinato al dispositivo collegato a quella porta: ciascuna interfaccia di rete riceve, quindi solo i pacchetti destinati al proprio indirizzo ed i pacchetti di broadcast.

L'impostazione della modalità promiscua è quindi insufficiente per poter intercettare il traffico in una rete gestita da switch. In questo caso ci si può collegare ad una porta chiamata "SPAN" nella terminologica di Cisco, "Roving Analysis" per 3Com e "port mirroring" per gli altri produttori che riceve il traffico circolante su tutte le porte dello switch.

Alcuni metodi per poter ricevere tutto il traffico dallo switch da una porta qualunque sono il MAC flooding, l'ARP poisoning e il port stealing.

Sniffing in reti geografiche

Per intercettare i dati che transitano su reti geografiche si utilizzano tecniche Man in the middle analoghe a quelle accennate in precedenza, operanti però a livello più alto: possono intervenire a livello di instradamento del traffico IP (routing) oppure inviare alle vittime informazioni fasulle per quanto riguarda la corrispondenza tra nomi a dominio e indirizzi IP sfruttando l'assenza di autenticazione del sistema DNS.

Modalità di difesa

- Una soluzione open source è ArpON [1] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.
- Cifratura del traffico, in particolare delle informazioni sensibili.
- Utilizzo di strumenti software in grado di rilevare la presenza di sniffer nella rete.
- Rafforzamento della sicurezza dei protocolli di rete.

Lo sniffing nella difesa del diritto d'autore

Lo sniffing pone problemi di privacy in quanto accede senza mandato e a insaputa dell'utente ad un computer che è sua proprietà privata nonché ad una rete che è proprietà di chi diffonde il software di accesso. In generale, l'accesso ad un'abitazione o altra proprietà privata per una perquisizione richiede un mandato della magistratura e che esso sia mostrato al proprietario del bene perquisito.

I dati forniti dall'Internet Service Provider non identificano la persona, ma l'utenza telefonica. Non necessariamente poi la persona che ha commesso il fatto è un componente del nucleo familiare, al quale è intestata l'utenza. Tramite un WISP o una rete wireless domestica è più facile che si verifichino violazioni della rete e accessi abusivi dall'esterno. La non-identificazione di chi commette materialmente il fatto esclude un nesso di causalità fra la connessione alla rete P2P e la violazione del diritto d'autore, e non è una prova sufficiente per gli effetti penali previsti dalla legge. Per l'ambito penale, serve un accertamento univoco e inequivocabile della persona e delle responsabilità. Tuttavia, il titolare della utenza telefonica può essere ritenuto responsabile della sua sicurezza e del suo utilizzo, e rispondere dell'illecito amministrativo.

La perquisizione dei domicili e l'accesso ai tabulati telefonici (dei provider per conoscere i siti visitati) sono provvedimenti riservati a illeciti penali. In Paesi come gli Stati Uniti, dove la violazione del copyright è punita con

sanzioni pecuniarie, è comunque diffusa tale prassi nelle indagini per violazioni del diritto d'autore.

Il codice penale italiano al cap.2 ("dei delitti in particolare") dedica un'apposita sezione a tale tema: "Dei delitti contro la inviolabilità del domicilio" (sez. IV). Gli artt. 615 bis e ter specificano le pene per accesso abusivo ad un sistema informatico o telematico, o interferenze illecite nella vita privata. Gli strumenti che controllano il traffico web di un utente, "si mettono in ascolto" su una porta del computer non utilizzata da alcun programma, e funzionano come uno "strumento di ripresa sonora" che registra tutto il traffico in ingresso e uscita dal nodo internet.

In questo caso è dato di sapere soltanto ciò che l'utente sta facendo con il browser Internet e con i programmi peer-to-peer, ma non con le altre applicazioni (se ad esempio sta ascoltando una canzone, vedendo un film, stampando un file). L'intrusione non consente un controllo o manipolazione del computer, ma comunque di "mantenervisi contro la volontà tacita di chi ha il diritto di escluderlo".

Entrando nelle reti di condivisione l'utente rende visibile una parte dei file del suo computer e inevitabilmente i file che sceglie di scaricare. Viene in questo modo a crearsi un conflitto con la normativa sulla privacy: la conservazione dei dati dei download, anche in forma aggregata e anonima, deve essere autorizzata nei confronti di chi immette file nelle reti P2P per "testarne" il gradimento del pubblico, oppure entra per perseguire in flagranza di reato chi viola i diritti di copyright.

A detta di alcuni giuristi l'accesso è più grave del reato di violazione del copyright che con esso si vuole reprimere. È stato osservato che è eccessivo uno sconfinamento nella giustizia penale e che l'entità della reclusione minima e massima non rispettano il proporzionalismo delle pene se comparate con le pene detentive di altri reati.

In questo senso, se può essere chiesto un risarcimento danni per la violazione del copyright, le persone oggetto di intercettazioni possono ottenere un risarcimento, probabilmente in misura maggiore, per la violazione dei loro diritti soggettivi.[2][3][4]

Note

[1] http://arpon.sf.net

[2] Una sentenza del Tribunale di Roma, del 17 marzo 2008, per il caso Peppermint/Techland/Logistep, è una delle prime in materia e crea un precedente giuridico. La casa discografica tedesca e un produttore di videogiochi polacchi si erano rivolti ad una società svizzera specializzata in intercettazioni nelle reti *peer-to-peer*. Rilevati gli indirizzi IP, le società ottengono dai *provider* italiani i nominativi corrispondenti, e inviano loro delle raccomandate nelle quali chiedono un risarcimento, riservandosi altrimenti ulteriori iniziative giudiziarie per la violazione del diritto d'autore. Il Tribunale di Roma rigetta le richieste di procedere, affermando che le società non hanno alcun diritto di accedere ai dati personali degli intercettati e che quindi i nominativi raccolti sono privi di valore probatorio, e non possono essere utilizzati in tribunale.

[3] Su esposto di una nota associazione dei consumatori, con un provvedimento del 28 febbraio 2008, pubblicato il 14 marzo, il Garante per la privacy, ha affermato che il trattamento dei dati personali è illegittimo poiché viola diversi principi: *finalità*, delle reti P2P destinate allo scambio di file e non alle intercettazioni; *trasparenza* e *buona fede*, essendo i dati prelevati senza informare gli interessati; *proporzionalità*: un diritto costituzionale come la segretezza nelle comunicazioni può essere limitato solo dall'esigenza di salvaguardare un diritto di pari rilevanza, quale non è il diritto d'autore. Secondo il Garante, il *discovery*, vale a dire la rivelazione delle generalità, violerebbe una sentenza della Corte di Giustizia Europea del 29 gennaio 2008, e tre sentenze della Corte Costituzionale italiana: la 372/2006 e la 38-349/2007.

[4] L'intercettazione limita diritti soggettivi della persona, la cui violazione in altri contesti costituisce reato, ed è utilizzata per accertare un illecito che è punito con un'ammenda. La sentenza del Tribunale di Roma afferma l'illegittimità delle intercettazioni in relazione a soggetti privati; il pronunciamento del Garante entra nel merito dichiarando l'uso delle intercettazioni nelle reti P2P illegittimo, al di là del soggetto che le opera. Il diritto alla riservatezza è disciplinato nel D. Lgs. n. 196 del 2003.

Bibliografia

- Alberto Ornaghi, Marco Valleri, *Man in the middle attacks* (http://www.blackhats.it/it/papers/Paper-mitm.pdf) (file pdf)

Voci correlate

- Cain & Abel
- Wireshark
- Xplico
- Firesheep
- Network tap
- Protocollo di rete
- Rete telematica

Altri progetti

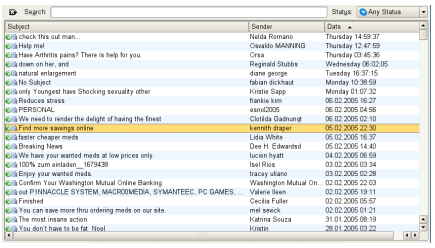
- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Computer data network analyzers

Collegamenti esterni

- ArpON home page (http://arpon.sourceforge.net) - ArpON (BSD)
- Wireshark (http://www.wireshark.org) - Wireshark (GPL)
- Wireshark (http://wiki.wireshark.org/CaptureSetup/Ethernet) - Wiki di Wireshark
- ettercap (http://ettercap.sourceforge.net/) - ettercap
- Packet sniffer (http://www.sniff-em.com) - Sniff-em
- TCP Dump (http://www.tcpdump.org) - TCP Dump (GPL)
- KSniffer (http://www.ksniffer.org/) - KSniffer (GPL)
- Xplico (http://www.xplico.org/) - Xplico (GPL)

Spam

Lo ***spamming***, detto anche **fare spam** o **spammare**, è l'invio di messaggi indesiderati (generalmente commerciali). Può essere attuato attraverso qualunque sistema di comunicazione, ma il più usato è Internet, attraverso messaggi di posta elettronica, chat, tag board o forum.



Una cartella di messaggi spam di KMail

Origine del termine

Spam (carne in scatoletta)

Il termine trae origine da uno sketch comico del Monty Python's Flying Circus ambientato in un locale nel quale ogni pietanza proposta dalla cameriera era a base di Spam (un tipo di carne in scatola). Man mano che lo sketch avanza, l'insistenza della cameriera nel proporre piatti con *Spam* («uova e Spam, uova pancetta e Spam, salsicce e Spam» e così via) si contrappone alla riluttanza del cliente per questo alimento, il tutto in un crescendo di un coro inneggiante allo *Spam* da parte di alcuni Vichinghi seduti nel locale.[1]

I Monty Python prendono in giro la carne in scatola Spam per l'assidua pubblicità che la marca era solita condurre. Nel periodo immediatamente successivo alla seconda guerra mondiale, questo alimento costava poco ed era parte integrante della dieta della famiglia tipica inglese, specialmente nella prima colazione per l'English breakfast.

Si ritiene che il primo spam via email della storia sia stato inviato il 1 maggio 1978 dalla DEC per pubblicizzare un nuovo prodotto, e inviato a tutti i destinatari ARPAnet della costa ovest degli Stati Uniti.[2]

Nella terminologia informatica le spam possono essere designate anche con il sintagma di junk-mail, che letteralmente significa posta-spazzatura, a rimarcare la sgradevolezza prodotta da tale molestia digitale.

Scopo

Il principale scopo dello spamming è la pubblicità, il cui oggetto può andare dalle più comuni offerte commerciali a proposte di vendita di materiale pornografico o illegale, come software pirata e farmaci senza prescrizione medica, da discutibili progetti finanziari a veri e propri tentativi di truffa. Uno **spammer**, cioè l'individuo autore dei messaggi spam, invia messaggi identici (o con qualche personalizzazione) a migliaia di indirizzi e-mail. Questi indirizzi sono spesso raccolti in maniera automatica dalla rete (articoli di Usenet, pagine web) mediante spambot ed appositi programmi, ottenuti da database o semplicemente indovinati usando liste di nomi comuni.

Per definizione lo spam viene inviato senza il permesso del destinatario ed è un comportamento ampiamente considerato inaccettabile dagli Internet Service Provider (ISP) e dalla maggior parte degli utenti di Internet. Mentre questi ultimi trovano lo spam fastidioso e con contenuti spesso offensivi, gli ISP vi si oppongono anche per i costi del traffico generato dall'invio indiscriminato.

Sondaggi hanno indicato che al giorno d'oggi lo spam è considerato uno dei maggiori fastidi di Internet; l'invio di questi messaggi costituisce una violazione del contratto "Acceptable Use Policy" (condotta d'uso accettabile) di

molti ISP e pertanto può portare all'interruzione dell'abbonamento (account) del mittente. Un gran numero di spammer utilizza intenzionalmente la frode per inviare i messaggi, come l'uso di informazioni personali false (come nomi, indirizzi, numeri di telefono) per stabilire account disponibili presso vari ISP. Per fare questo vengono usate informazioni anagrafiche false o rubate, in modo da ridurre ulteriormente i loro costi. Questo permette di muoversi velocemente da un account a un altro appena questo viene scoperto e disattivato dall'ISP. Gli spammer usano software creato per osservare connessioni Internet con scarsa sicurezza, che possono essere facilmente dirottate in modo da immettere i messaggi di spam direttamente nella connessione dell'obiettivo con il proprio ISP. Questo rende più difficile identificare la posizione dello spammer e l'ISP della vittima è spesso soggetto di aspre reazioni e rappresaglie da parte di attivisti che tentano di fermare lo spammer. Entrambe queste forme di spamming "nascosto" sono illegali, tuttavia sono raramente perseguiti per l'impiego di queste tattiche.

I mittenti di e-mail pubblicitarie affermano che ciò che fanno non è spamming. Quale tipo di attività costituisca spamming è materia di dibattiti, e le definizioni divergono in base allo scopo per il quale è definito, oltre che dalle diverse legislazioni. Lo spamming è considerato un reato in vari paesi e in Italia l'invio di messaggi non sollecitati è soggetto a sanzioni.

Altri termini

I termini *unsolicited commercial email*, UCE (email commerciale non richiesta) e *unsolicited bulk email*, UBE (email non richiesta in grandi quantità) sono usati per definire più precisamente e in modo meno gergale i messaggi e-mail di spam. Molti utenti considerano tutti i messaggi UBE come spam, senza distinguere il loro contenuto, ma i maggiori sforzi legali contro lo spam sono effettuati per prendere di mira i messaggi UCE. Una piccola ma evidente porzione di messaggi non richiesti è anche di carattere non commerciale; alcuni esempi comprendono i messaggi di propaganda politica e le catene di Sant'Antonio

Spamming attraverso E-Mail

I più grandi ISP come America OnLine [3] riferiscono che una quantità che varia da un terzo a due terzi della capacità dei loro server di posta elettronica viene consumata dallo spam. Siccome questo costo è subito senza il consenso del proprietario del sito, e senza quello dell'utente, molti considerano lo spam come una forma di furto di servizi. Molti spammer mandano i loro messaggi UBE attraverso gli open mail relay. I server SMTP, usati per inviare e-mail attraverso internet, inoltrano la posta da un server a un altro; i server utilizzati dagli ISP richiedono una qualche forma di autenticazione che garantisca che l'utente sia un cliente dell'ISP. I server open relay non controllano correttamente chi sta usando il server e inviano tutta la posta al server di destinazione, rendendo più difficile rintracciare lo spammer.

Un punto di vista "ufficiale" sullo spamming può essere trovato nel RFC 2635.

Spamming per interposta persona

Lo spamming per interposta persona è un mezzo più subdolo utilizzato sfruttando l'ingenuità di molta gente. Per l'esattezza si intende di solito l'invio di Email commerciali ad alcuni destinatari conosciuti e magari regolarmente iscritti ad una newsletter dello spammer invitandoli a far conoscere una certa promozione ad uno o più persone conosciute dall'ingenuo destinatario, invogliandolo magari con qualche piccolo compenso.

Grazie a questo sistema sarà l'ingenuo destinatario a "spammare" altre caselle di posta di suoi conoscenti e quindi coprendo colui che c'è dietro e che guadagnerà da questo comportamento.

I costi

Lo spamming è a volte definito come l'equivalente elettronico della posta-spazzatura (junk mail). Comunque, la stampa e i costi postali di questa corrispondenza sono pagati dal mittente - nel caso dello spam, il server del destinatario paga i costi maggiori, in termini di banda, tempo di elaborazione e spazio per immagazzinamento. Gli spammer usano spesso abbonamenti gratis, in modo tale che i loro costi siano veramente minimi. Per questa ricaduta di costi sul destinatario, molti considerano questo un furto o un equivalente di crimine. Siccome questa pratica è proibita dagli ISP, gli spammer spesso cercano e usano sistemi vulnerabili come gli open mail relay e server proxy aperti. Essi abusano anche di risorse messe a disposizione per la libera espressione su internet, come remailer anonimi. Come risultato, molte di queste risorse sono state disattivate, negando la loro utilità agli utenti legittimi. Molti utenti sono infastiditi dallo spam perché allunga i tempi che usano per leggere i loro messaggi di e-mail.

Economia

Siccome lo spam è economico da inviare, un ristretto numero di spammer può saturare Internet con la sua spazzatura. Nonostante che solo un piccolo numero dei destinatari sia intenzionato a comprare i prodotti, ciò consente agli spammer di mantenere questa pratica attiva. Inoltre, sebbene lo spam appaia per una azienda rispettabile una via economicamente non attuabile per fare business, è sufficiente per gli spammer professionisti convincere una piccola porzione di inserzionisti ingenui che è efficace per fare affari.

Difese contro lo spam

È presente un certo numero di servizi e software, che spesso sono chiamati **antispam**, e che i server e-mail e gli utenti possono utilizzare per ridurre il carico di spam sui loro sistemi e caselle di posta. Alcuni di questi contano sul rifiuto dei messaggi provenienti dai server conosciuti come spammer. Altri analizzano in modo automatico il contenuto dei messaggi e-mail ed eliminano o spostano in una cartella speciale quelli che somigliano a spam. Questi due approcci al problema sono talvolta definiti come *bloccaggio* e *filtraggio*. Ognuna delle tecniche ha i suoi difensori e vantaggi; mentre entrambe riducono l'ammontare di spam inviata alle caselle postali degli utenti, il bloccaggio permette di ridurre la banda sprecata, rifiutando i messaggi prima che siano trasmessi al server dell'utente. Il filtraggio tende ad essere una soluzione più accurata, poiché può esaminare tutti i dettagli del messaggio. Molti sistemi di filtraggio si avvantaggiano delle tecniche di apprendimento del software, che permette di aumentare la propria accuratezza rispetto al sistema manuale. Alcuni trovano questa tecnica troppo invadente nei riguardi della privacy, e molti amministratori preferiscono bloccare i messaggi che provengono dai server tolleranti nei confronti degli spammer.

DNSBL

Una specifica tecnica di bloccaggio comprende le DNSBL (DNS-based blackhole lists), nella quale un server pubblica liste di indirizzi ip, in modo che un server di posta possa essere facilmente impostato per rifiutare la posta che proviene da questi indirizzi. Ci sono diverse liste di DNSBL, che hanno politiche diverse: alcune liste contengono server che emettono spam, altre contengono open mail relay, altre elencano gli ISP che supportano lo spam.

Filtraggio statistico ed euristico

Fino a poco tempo fa, le tecniche di filtraggio facevano affidamento agli amministratori di sistema che specificavano le liste di parole o espressioni regolari non permesse nei messaggi di posta. Perciò se un server riceveva spam che pubblicizzava "herbal Viagra", l'amministratore poteva inserire queste parole nella configurazione del filtro. Il server avrebbe scartato tutti i messaggi con quella frase. Lo svantaggio di questo filtraggio "statico" consiste nella difficoltà di aggiornamento e nella tendenza ai falsi positivi: è sempre possibile che un messaggio non-spam contenga quella frase. Il filtraggio euristico, come viene implementato nel programma SpamAssassin, si basa nell'assegnare un

punteggio numerico a frasi o modelli che si presentano nel messaggio. Quest'ultimo può essere positivo, indicando che probabilmente contiene spam o negativo in caso contrario. Ogni messaggio è analizzato e viene annotato il relativo punteggio, esso viene in seguito rifiutato o segnalato come spam se quest'ultimo è superiore ad un valore fissato. In ogni caso, il compito di mantenere e generare le liste di punteggi è lasciato all'amministratore.
Il filtraggio statistico fa uso di quelli che sono chiamati filtri bayesiani. Fu proposto per la prima volta nel 1998 nel AAAI-98 Workshop on Learning for Text Categorization, e fu reso popolare da un articolo di Paul Graham nel 2002. Esso usa metodi probabilistici, ottenuti grazie al Teorema di Bayes, per predire se un messaggio è spam o no, basandosi su raccolte di email ricevute dagli utenti.

Tecniche miste

Da qualche tempo stanno crescendo vari sistemi di filtraggio che uniscono più tecniche di riconoscimento dello spam, in modo da un lato minimizzare il rischio di falsi positivi (ovvero email regolari scambiate erroneamente per spam), dall'altro per aumentare l'efficienza del filtraggio. Si può quindi pensare di combinare il filtraggio per DNSBL con quello euristico e statistico, come alcuni programmi iniziano a prevedere, e fare così in modo di unire i pregi di ogni metodo di filtraggio e contemporaneamente ridurre i rischi grazie ai controlli multipli.

I comportamenti contro lo spam

A parte l'installazione di software di filtraggio dalla parte degli utenti, essi possono proteggersi dall'attacco dello spam in molti altri modi.

Address munging

Un modo in cui gli spammer ottengono gli indirizzi e-mail è il setaccio del Web e di Usenet per stringhe di testo che assomigliano a indirizzi. Perciò se l'indirizzo di una persona non è mai apparso in questi posti, non potrà essere trovata. Un sistema per evitare questa raccolta di indirizzi è falsificare i nomi e indirizzi di posta. Gli utenti che vogliono ricevere in modo legittimo posta riguardante il proprio sito Web o i propri articoli di Usenet possono alterare i loro indirizzi in modo tale che gli esseri umani possano riconoscerli ma i software degli spammer no. Per esempio, `joe@example.net` potrebbe venir modificato in `joeNOS@PAM.example.net`. Questo sistema è detto *address munging*, dalla parola "munge" tratta dal Jargon File che significa rompere. Questo sistema, comunque, non sfugge ai cosiddetti "attacchi al dizionario" nei quali lo spammer genera un numero di indirizzi che potrebbero esistere, come `adam@aol.com` che, se esistesse, riceverebbe molto spam.

Bug e Javascript

Molti programmi di posta incorporano le funzionalità di un Web browser come la visualizzazione di codice HTML e immagini. Questa caratteristica può facilmente esporre l'utente a immagini offensive o pornografiche contenute nelle e-mail di spam. In aggiunta, il codice HTML potrebbe contenere codice JavaScript per dirigere il browser dell'utente ad una pagina pubblicitaria o rendere il messaggio di spam difficile o impossibile da chiudere o cancellare. In alcuni casi, messaggi del genere contenevano attacchi ad alcune vulnerabilità che permettevano l'installazione di programmi di tipo spyware (alcuni virus informatici sono prodotti attraverso gli stessi meccanismi). Gli utenti possono difendersi utilizzando programmi di posta che non visualizzano HTML o allegati o configurarli in modo da non visualizzarli di default.

Evitare di rispondere

È ben noto che alcuni spammer considerano le risposte ai loro messaggi - anche a quelle del tipo "Non fare spam" - come conferma che l'indirizzo è valido e viene letto. Allo stesso modo, molti messaggi di spam contengono indirizzi o link ai quali viene indirizzato il destinatario per essere rimosso dalla lista del mittente. In svariati casi, molte persone che combattono lo spam hanno verificato questi collegamenti e confermato che non portano alla rimozione dell'indirizzo, ma comportano uno spam ancora maggiore.

Denunciare spam

Agli ISP

La maggioranza degli ISP proibisce esplicitamente ai propri utenti di fare spam e in caso di violazione essi vengono espulsi dai loro servizi. Rintracciare l'ISP di uno spammer e denunciarlo spesso porta alla chiusura dell'abbonamento. Sfortunatamente, questo può essere difficile e anche se ci sono degli strumenti che possono aiutare, non sempre sono accurati. Tre di questi servizi sono SpamCop [4],Network Abuse Clearinghouse [5] e [6] Essi forniscono mezzi automatici o semi automatici per denunciare spam agli ISP. Alcuni li considerano imprecisi rispetto a ciò che può fare un esperto di posta elettronica, ma molti utenti non sono così esperti.

Gli ISP spesso non mettono in atto misure preventive per impedire l'invio di spam, quali un limite massimo agli indirizzi di posta ai quali inoltrare la stessa e-mail, e un limite dell'ordine delle migliaia di unità alla posta elettronica inviabili in un giorno.

Talora, oltre all'accesso viene disattivata la connessione Internet. La disconnessione può essere permanente se l'abbonamento è ADSL a IP statico, bloccando l'indirizzo IP.

Alle Autorità

Il metodo più efficace per fermare gli spammer è di sporgere reclamo alle autorità competenti. Questo richiede maggiori tempo ed impegno ma gli spammer vengono perseguiti a norma di legge e pagano eventuali multe e risarcimenti, in questo modo per loro si annulla il vantaggio economico, anzi l'azione illecita si traduce in una perdita economica.

Le procedure da intraprendere:

1. Individuare gli indirizzi in rete da dove proviene lo spam tramite per esempio: SpamCop [4] o Network Abuse Clearinghouse [5]

2. Individuare lo stato dal quale è stato spedito lo spam per esempio tramite MostraIP [7]

3. Verificare se lo stato in oggetto mette a disposizione un indirizzo di posta elettronica per esempio dalle liste pubblicate su OECD Task Force on Spam [8], Spam Reporting Adresses [9] o Spam Links [10].

Altre forme di spam

Fino dal 1990, gli amministratori di sistema hanno compiuto molti sforzi per fermare lo spam, alcuni dei quali con esiti positivi. Come risultato, coloro che inviano messaggi di spam si sono rivolti ad altri mezzi.

WikiWikiWeb

Tutti i siti web che utilizzano il sistema wiki, come ad esempio Wikipedia, che dà ampie possibilità a un visitatore di modificare le proprie pagine, sono un bersaglio ideale per gli spammer, che possono avvantaggiarsi dell'assenza di un controllo continuo sul contenuto introdotto, per inserire i propri link pubblicitari. Sono stati creati filtri che impediscono la pubblicazione di determinati link proprio per ovviare a questo fenomeno. In molti casi lo scopo è quello di ottenere un miglioramento della visibilità del proprio sito sui motori di ricerca.

Su Wikipedia questo fenomeno viene contrastato in modo deciso: i link esterni sono accompagnati dall'attributo "nofollow", che indica ai motori di ricerca di non seguire il link; le voci vengono ripristinate alla loro versione precedente all'intervento; in caso di reiterati inserimenti, l'indirizzo IP viene bloccato in scrittura.

Messaging spam

I sistemi di instant messaging sono un obiettivo comune tra gli spammer. Molti sistemi di messaging pubblicano il profilo degli utenti, includendo informazioni demografiche come l'età e il sesso. Coloro che fanno pubblicità possono impiegare queste informazioni, inserirsi nel sistema e mandare spam. Per contrastare ciò, alcuni utenti scelgono di ricevere messaggi solo dalle persone che conoscono. Nel 2002, gli spammer hanno iniziato usando il servizio di messaging integrato in Microsoft Windows, winpopup, che non è "MSN Messenger", ma piuttosto una funzione progettata per permettere ai server di inviare avvertimenti agli utenti delle workstation. I messaggi appaiono come delle normali dialog box e possono essere inviati usando qualunque porta NetBIOS, per questo il blocco delle porte provocate da un firewall comprende le porte da 135 a 139 e 445.

Usenet

Le vecchie convenzioni di Usenet definiscono erroneamente lo spamming come "eccessivo invio multiplo di messaggi" (messaggi sostanzialmente simili la quale definizione esatta è flooding). Nei primi anni '90 ebbe luogo una notevole controversia tra gli amministratori di server news sull'uso dei messaggi di cancellazione per il controllo dello spam. Un messaggio di cancellazione è un'istruzione ad un server delle news per cancellare un messaggio, in modo da renderlo inaccessibile a chi lo volesse leggere. Alcuni lo considerano un cattivo precedente, incline alla censura, mentre altri lo ritengono uno strumento giusto per controllare la crescita del problema dello spam. In quel periodo, dovunque il termine spam su Usenet era usato per riferirsi all'invio di messaggi multipli. Furono coniati altri termini per comportamenti simili, come un cross-posting eccessivo o pubblicità non in tema con il manifesto del newsgroup, comunque più recentemente anche questi casi sono stati catalogati con il termine spam per analogia al ben più conosciuto fenomeno della posta elettronica.

Forum

Nei forum (o BBS) spesso per spam si intende l'invio di link riferiti ad altri forum per fare arrivare utenti, molto spesso è possibile caricare la medesima discussione nello stesso forum per attirare ancora più utenti. Altre volte si intendono erroneamente come "spam" anche i messaggi inutili e/o privi di un qualsivoglia senso logico; in questo caso, tuttavia, il termine più adatto sarebbe "flood".

L'utente che pratica **spam** nei forum, soprattutto nel secondo caso, viene tipicamente definito con il termine gergale **spammone**.

Il termine è dispregiativo, un utente considerato spammone viene spesso giudicato anche inaffidabile o incompetente dagli altri. A volte però il termine può avere un tono più scherzoso e goliardico, soprattutto nei forum dove c'è abbastanza tolleranza nei confronti dello spam.

Blog

Con l'avvento ed il successo riscosso dai blog, non potevano mancare tecniche di spamming che riguardano anche questa nuova recente categoria di media. Oltre al semplice posting di link che reindirizzano il visitatore sui siti che lo spammer vuole pubblicizzare, esistono due tecniche, ben più evolute: lo spammer fa uso di una sorta di *query-bombing* dei sistemi multipiattaforma più noti come WordPress[11] o b2evolution[12], attaccando i database con l'inserimento continuo di messaggi pubblicitari. Le componenti di un blog più vulnerabili sono quindi quelle che sono esposte all'utilizzo pubblico: i *commenti* (per i quali i vari creatori dei sistemi multipiattaforma forniscono con periodicità plug-in di protezione) e gli *hitlogs*, ovvero il sistema di tracking dei referer (i siti che linkano la pagina in questione).

Keyword spamming

Il *keyword spamming* è il termine dato all'eccessivo uso di *keyword* o parole chiave in una pagina web al fine di incrementarne la visibilità per i motori di ricerca. Questa tecnica è considerata una cattiva SEO.

Le nuove tecniche ed algoritmi hanno però introdotto delle funzionalità che permettono ai motori di controllare l'utilizzo ripetitivo degli stessi termini e quindi penalizzare i siti web che adottano questa forma di spam.

Aspetti giuridici

Lo spam è un reato in innumerevoli paesi, inquisito anche all'estero con richieste di estradizione. Tra gli *spammer* più famosi, si ricordano Laura Betterly, Brian Haberstroch, Leo Kuvayevo, Jeremy Jaynes e Sanford Wallacer.

Italia

La disciplina italiana concernente l'invio di posta elettronica a fini commerciali è disciplinata dall'**art. 130 Codice Privacy**, rubricato "Comunicazioni indesiderate". L'ambito di applicazione di detto articolo è proprio quello dello spamming, seppur la rubrica si limiti a parlare di comunicazioni indesiderate e non menzioni quelle semplicemente non richieste. Il modello di regolazione scelto dal legislatore italiano (e in generale da tutti gli stati aderenti alla Comunità Europea) è quello dell'*opt-in*, che prevede la possibilità di avvalersi del trattamento dei dati personali solo dopo aver ottenuto il consenso del soggetto interessato.

È inoltre vietato, sempre dall'art. 130 Codice Privacy, l'invio di comunicazioni a scopi pubblicitari, per la vendita diretta o per ricerche di mercato effettuato camuffando o celando l'identità del mittente o ancora senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i propri diritti. È però prevista una deroga ai dettami di tale articolo, che consente di utilizzare le coordinate di posta elettronica, fornite dall'interessato nel contesto della vendita di un prodotto o servizio, per l'invio di ulteriori messaggi promozionali aventi ad oggetto simili beni o servizi, senza dover nuovamente chiederne il consenso.

Vi è poi nel nostro ordinamento un'ulteriore disposizione al riguardo, rinvenibile nel **d.lgs. 9 aprile 2003, n.70** sul commercio elettronico. L'art. 9 afferma infatti che le comunicazioni commerciali non sollecitate trasmesse da un prestatore per posta elettronica devono, in modo chiaro ed inequivocabile, essere identificate come tali fin dal momento in cui il destinatario le riceve e devono altresì contenere l'indicazione che il destinatario del messaggio può opporsi al ricevimento in futuro di tali comunicazioni.

Va da ultimo esaminato l'impianto sanzionatorio previsto dal nostro ordinamento. Anzitutto lo stesso art. 130 comma 6 attribuisce al Garante per la protezione dei dati personali, in caso di reiterata violazione delle disposizioni previste in tale ambito, il potere di provvedere, negli ambiti di un procedimento di reclamo attivato, tramite prescrizione ai fornitori di servizi di comunicazione elettronica (ISP), adottando misure di filtraggio o altre misure praticabili nei confronti di un certo indirizzo di posta elettronica.

Di ben maggiore deterrenza appare poi l'**art. 167 del Codice Privacy**, nel quale si prevede che, salvo il fatto non costituisca più grave reato, chiunque proceda al trattamento dei dati personali in violazione di quanto previsto nel Codice stesso, al fine di trarne un profitto o recare ad altri un danno, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione di tali dati, con la reclusione da sei a ventiquattro mesi. L'attività di spamming espone, infine, ai sensi dell'**art. 161 Codice Privacy**, alla sanzione amministrativa di omessa informativa (di cui all'art 13), la quale va da un minimo di tremila euro ad un massimo di diciottomila euro. La sanzione viene erogata dall'autorità Garante per la protezione dei dati personali a seguito di un apposito ricorso ai sensi degli artt. 145 ss. Codice Privacy; tale ricorso che non può essere proposto se, per il medesimo oggetto e tra le medesime parti, è già stata adita l'autorità giudiziaria.

La tutela amministrativa risulta dunque essere alternativa a quella giudiziaria, inutile dire che risulta essere anche meno soddisfacente (dal punto di vista economico) per chi se ne avvale, lasciando quindi un ruolo preminente a quella giudiziaria. La prima controversia italiana avente ad oggetto attività di spamming è stata risolta dal Giudice di

Pace di Napoli, che, con sentenza 26 giugno 2004, ha riconosciuto l'illiceità di tale attività, condannando il titolare del trattamento al risarcimento del danno patrimoniale, non patrimoniale, esistenziale e da stress subito dal titolare della casella di posta elettronica.

L'assetto che deriva dalle regole appena esposte, in piena coerenza con la vigente disciplina nazionale sulla data protection, qualifica dunque il nostro come un sistema improntato al cosiddetto "opt-in" (necessità del consenso preventivo), salvo il temperamento relativo alla comunicazione via e-mail finalizzata alla vendita di "propri prodotti o servizi analoghi", ispirato ad un sistema che potremmo definire di "soft opt-out". Con particolare riferimento al tema delle comunicazioni commerciali, l'art. 58 del Codice del consumo, D.Lgs. 206 del 2005, raccogliendo integralmente il disposto del pre-vigente D.Lgs. 185/99, ha introdotto tuttavia delle norme sostanzialmente differenti ove prevede particolari limiti all'impiego di alcune tecniche di comunicazione a distanza: 1.l'impiego da parte di un professionista del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore; 2.tecniche di comunicazione a distanza diverse da quelle di cui al comma 1, qualora consentano una comunicazione individuale, possono essere impiegate dal fornitore se il consumatore non si dichiara esplicitamente contrario. Mentre il primo comma prevede un sistema pienamente assimilabile all'opt-in, il secondo è invece apertamente ispirato ai meccanismi dell'opt-out. Questa regolamentazione comportava già alcuni gravi dubbi interpretativi, soprattutto per i riflessi operativi che ne derivavano: che relazione intercorre tra il consenso richiesto dalla normativa privacy e quello imposto dall'art. 58, comma 1, del Codice del consumo? Il tema è ancora oggi fortemente dibattuto, fermi però alcuni punti di riferimento che devono costituire i criteri guida per la soluzione di questo problema esegetico: a) si tratta di due consensi aventi natura diversa, per il semplice fatto che tutelano interessi diversi (quello alla riservatezza da un lato, e quello alla correttezza del comportamento del professionista dall'altro); b) comuni sono le sanzioni che derivano dalla violazione delle norme, come evidentemente dimostrato dall'art. 62 del Codice del consumo, che espressamente prevede la trasmissione al Garante Privacy del verbale ispettivo redatto dagli organi competenti a rilevare le violazioni dei diritti dei consumatori, affinché il Garante stesso irroghi le diverse sanzioni prescritte dal Codice privacy. Qualsiasi scelta nella impostazione della modulistica necessaria alla acquisizione del consenso, deve tenere dunque ben presenti la tratteggiata distinzione. Si deve comunque sottolineare che in questo tema e in virtù di quanto prima sostenuto in tema di sanzioni debba ritenersi più significativo l'orientamento del Garante Privacy il quale, in numerosi provvedimenti, ha dichiarato l'illegittimità di qualsiasi comunicazione non preventivamente autorizzata: RILEVATO che ai sensi dell'art. 130 del Codice (salvo quanto previsto dal comma 4 del medesimo articolo) il consenso preventivo degli interessati è richiesto anche per l'invio di una sola comunicazione mediante posta elettronica volta ad ottenere il consenso per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale o, comunque, per fini promozionali (come quella contestata volta a rendere noti i servizi offerti attraverso un sito Internet) (Provvedimento del 20 dicembre 2006).

Stati Uniti

Dal 1997 in poi si registra negli Stati Uniti un'intensa attività a livello legislativo statale in risposta ai problemi creati dal crescente fenomeno della posta indesiderata.

Trentasei stati hanno emanato una legislazione *ad hoc* sul tema. Le previsioni legislative dei singoli stati sono le più disparate, alcuni dispongono che vi debbano necessariamente essere informazioni atte ad identificare il mittente, unanime è poi la previsione della possibilità per l'utente di vedere cancellato il proprio indirizzo dalla banca dati dello spammer. Gli Stati Uniti infatti aderiscono al modello di regolazione *opt-out* (fatta eccezione per lo stato della California e del Delaware), che di fatto rende lecito lo spamming ma consente all'utente di esprimere in ogni momento la propria volontà a che cessi l'attività di spamming sulla sua casella di posta elettronica.

Altre previsioni legislative statali generalmente condivise riguardano il divieto di porre in essere, mediante lo spamming, attività ingannevoli, falsificando alcune parti del messaggio o l'oggetto stesso. Dal momento che la quasi totalità dei messaggi è spedita in maniera transfrontaliera all'interno della federazione, si è resa necessaria

un'armonizzazione tra le varie legislazioni. Alcune legislazioni statali contengono infatti delle previsioni atte ad individuare l'ordinamento competente a regolare i vari casi di spamming che coinvolgono più stati.

L'intervento più significativo e uniformante però è avvenuto a livello federale, con il **Can-Spam Act del 2003** (entrato in vigore il primo gennaio 2004). Con questo provvedimento si rimette al Dipartimento di Giustizia, lo FTC, all'attourney general statale e agli ISP la facoltà di tutelare i diritti dei privati, stabilendo per coloro che violano le previsioni dello statute (tra le quali, ancora, l'inserimento di informazioni e oggetti fuorvianti o l'omissione dell'apposita etichetta prevista per i messaggi a contenuto sessuale) sanzioni pecuniarie fino a $ 2.000.000, con la possibilità di triplicare la pena nel caso in cui la violazione sia stata commessa intenzionalmente e consapevolmente. Sono previste inoltre sanzioni penali per gli spammer che inviano messaggi commerciali illeciti, a contenuto osceno, pedo-pornografico o l'identità del cui mittente è falsa o rubata. Il Can-Spam Act prevale sulle disposizioni normative statali, ma di fatto, è stato tacciato dalla dottrina come statute per lo più "simbolico" alla luce del suo scarso impatto pratico.

Software e servizi on-line contro lo spam

Software

- Avira
- Spamassassin
- BarracudaNetworks
- ClearSWIFT
- Endian
- GFI
- IronPort
- Kaspersky
- Sinapsi Antispam
- SonicWall
- Sophos
- Stevtech
- SPAMfighter
- Symantec
- Antispameurope
- Abaca Technology Corporation

Note

[1] http://it.youtube.com/watch?v=anwy2MPT5RE Lo sketch originale su YouTube.

[2] http://www.templetons.com/brad/spamreact.html Pagina che riporta le reazioni al primo spam, e una trascrizione di quest'ultimo; notare come, non essendo in grado il programma di invio di posta elettronica di supportare più di un certo numero di indirizzi email, parte di questi ultimi siano finiti nel corpo della mail.

[3] http://www.aol.com

[4] http://spamcop.net

[5] http://www.abuse.net/

[6] http://www.spammer.org/spammer

[7] http://www.mostraip.it/Default.aspx

[8] http://www.oecd-antispam.org/sommaire.php3

[9] http://banspam.javawoman.com/report3.html

[10] http://spamlinks.net/track-report-addresses.htm#country

[11] WordPress › Blog Tool and Publishing Platform (http://wordpress.org)

[12] b2evolution.org (http://b2evolution.org)

Bibliografia

- "Diritto dell'informatica e della comunicazione", A.M. Gambino, A. Stazi, con la collaborazione di D. Mula, Giappichelli editore, 2009 (http://www.dimt.it/Segnalazioni editoriali.html)

Voci correlate

- E-mail
- Mailbombing

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Electronic spam
- **Wikizionario** contiene la voce di dizionario: http://it.wiktionary.org/wiki/Spam

Collegamenti esterni

- Trascrizione della scenetta dei Monty Python (http://www.spamterminator.it/orig_it.asp)
- Progetto Spamhaus (http://www.spamhaus.org)
- Spam Laws - Leggi sullo spam di diverse nazioni (http://www.spamlaws.com/)
- Un filtro antispam intelligente in Java (http://www2.mokabyte.it/cms/article.run?articleId=STS-3CY-GIV-6HP_7f000001_14191084_d2ba6e6c)

Spoofing

Lo **spoofing** è un tipo di attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (spoof). Lo spoofing può avvenire in qualunque livello della pila ISO/OSI e oltre: può riguardare anche la falsificazione delle informazioni applicative. Quando la falsificazione dell'identità non avviene in campo informatico si parla di social engineering.

Tipologie di spoofing

Esistono diversi tipi di attacchi spoofing a diversi livelli della pila OSI, ma in ogni caso si tratta di far credere alla vittima che si è qualcosa di diverso: un hostname, un indirizzo ethernet o altro ancora.

Spoofing a livello 2

Quando l'informazione falsificata è un indirizzo MAC si parla di MAC-spoofing. L'attacco consiste nell'immettere in rete un pacchetto che contiene un MAC address diverso da quello dell'attaccante ed uguale a quello della vittima, con lo scopo di effettuare un attacco. Un esempio di questa tecnica viene impiegata nel MAC flooding in cui un attaccante manda continuamente pacchetti in rete con un MAC che non è il suo. Questo attacco ha l'effetto di saturare il forwarding database dello switch causandone malfunzionamenti cioè forzando il successivo broadcast in tutta la rete. Un altro attacco di tipo MAC-Spoofing è il port stealing in cui l'uso da parte di un attaccante di un MAC Address di un host vittima è finalizzato al furto della porta dello switch dedicata all'host vittima. Un attacco che riguarda la sicurezza del layer 2 ma non direttamente il mac spoofing è l'ARP poisoning mentre un tool per prevenire e bloccare questo attacco è ArpON [1] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering

come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.

Spoofing a livello 3

Quando l'informazione falsificata è un indirizzo IP si parla di IP spoofing. In generale è semplice falsificare un indirizzo in quanto il protocollo non implementa alcun sistema di sicurezza. In questo caso si assiste ad un routing asimmetrico visto che il pacchetto di risposta a quello falsificato verrà inviato al vero IP. Gli ISP possono attivare diversi sistemi di sicurezza per impedire l'IP spoofing. Il primo metodo consiste nell'impedire che da una interfaccia (di un router/firewall) vengano inviati pacchetti in cui l'IP sorgente non è quello che ci si aspetta. Il secondo metodo consiste nell'uso delle tabelle di routing. Se l'interfaccia di provenienza per un pacchetto non è la stessa che verrebbe scelta dal router per l'inoltro del pacchetto di risposta allora questo pacchetto viene scartato. Questo sistema si chiama **uRPF**[1].

Spoofing a livello 4

Il livello 4 della pila ISO/OSI non è rilevante in fase di autenticazione, quindi non si parla di UDP/TCP spoofing, ma di un attacco di IP-spoofing portato verso uno di questi due protocolli.

Spoofing UDP

È analogo al caso IP. Essendo UDP un protocollo connectionless la falsificazione di un datagram UDP consiste nell'immettere le informazioni desiderate e falsificare l'header.

Spoofing TCP

Lo spoofing di una sessione TCP è decisamente più complesso del caso UDP. TCP è infatti un protocollo connection oriented che richiede che venga stabilita una sessione tramite il three way handshake. Se viene forgiato un pacchetto SYN con l'indirizzo IP falsificato e questo viene inviato ad un server, prima che sia possibile inviare i dati il server cercherà di portare a termine l'handshake rispondendo con un pacchetto SYN/ACK. Questo pacchetto riporterà l'indirizzo IP falsificato quindi non verrà inviato indietro all'attaccante che quindi non potrà rispondere con il terzo e ultimo pacchetto (il pacchetto ACK). Per portare a termine questo attacco è necessario inviare un pacchetto ACK al server che riporti nuovamente l'indirizzo IP falsificato, ma anche il sequence number che il server ha inserito nel pacchetto SYN/ACK. Per scegliere questo numero l'attaccante deve sapere come il server li sceglie. Siccome l'attaccante invia il primo e il terzo pacchetto senza vedere il secondo, questo attacco si chiama **blind spoofing**. Una trattazione approfondita sulla predizione dei numeri di sequenza viene fatta da lcamtuf in [2] e in [3].

Spoofing applicativo

Con spoofing applicativo si intendono quelle tecniche di spoofing destinate a colpire i protocolli di livello applicativo (layer 7 della pila ISO/OSI) o le applicazioni stesse.

WEB Spoofing

Quando lo spoofing coinvolge il web (server applicativo, host server o protocolli web) si parla di web spoofing. Nell'accezione più comune il web spoofing riguarda la falsificazione di un server web per far credere ad un utente di essere connesso ad un certo server mentre è connesso ad un server malevolo.

Descriviamo in primis la tecnica nel caso in chiaro (non TLS). La prima azione che deve effettuare un attaccante per redirigere un client verso un server falso (anche chiamato shadow server o server ombra) è di falsificare l'associazione tra l'indirizzo web e l'indirizzo IP. Questa operazione viene effettuata tramite un attacco di dns poisoning. A questo punto l'attaccante ha fatto credere al client che l'indirizzo del server vero è quello invece del server falso. L'attaccante ha costruito in precedenza un server falso che può

- contenere una copia del server vero (ogni pagina è stata copiata in locale sul server ombra)

- rigirare pagina per pagina le connessioni del client verso il server vero

In entrambi questi casi quello che ottiene l'attaccante è di fingersi il server vero, catturando credenziali di accesso, per esempio. La creazione dello shadow server è uguale a ciò che si fa nel phishing, ma in questo caso c'è stato un preventivo attacco diretto al client.

Nel caso TLS la cosa si complica notevolmente in quanto bisogna violare il sistema crittografico di TLS. Siccome gli algoritmi stessi sono difficilmente violabili, un attaccante opera un attacco a metà tra l'informatica e il social engineering. L'attacco si svolge in tutto e per tutto come il caso senza TLS, ma l'opzione scelta è quella di rigirare le connessioni verso il server vero. Quando il client riceve il certificato del server esso dovrebbe verificarne l'autenticità. L'attaccante quindi genera un certificato server falso, totalmente uguale al certificato vero, solamente che non è firmato dalla stessa CA. L'utente quindi riceve un certificato che a prima vista è valido e solo un'analisi approfondita rivela la sua falsità. L'attaccante potrebbe rendere ancora più ardua l'identificazione usando una CA falsa, ma uguale a quella vera (cioè con stessi nomi, identificativi, ecc.). Se l'utente non è sufficientemente a conoscenza della problematica può cliccare per accettare anche se la prova crittografica non è completa. A questo punto il server dell'attaccante fa una connessione verso il server vero agendo da proxy e intercettando le comunicazioni. Questo è un attacco di tipo man in the middle. Alcuni tool che offrono la possibilità di fare questo attacco sono dsniff[4] ed ettercap[5] mentre un tool per prevenire e bloccare questo attacco è ArpON [1] "ARP handler inspection". ArpON è un demone portabile che rende il protocollo ARP sicuro contro attacchi Man in The Middle (MITM) attraverso tecniche ARP Spoofing, ARP Cache Poisoning, ARP Poison Routing (APR). Blocca anche attacchi derivati quali Sniffing, Hijacking, Injection, Filtering come: DHCP Spoofing, DNS Spoofing, WEB Spoofing, Session Hijacking e SSL/TLS Hijacking & co attacks.

Note

[1] (**EN**) Understanding Unicast Reverse Path Forwarding (http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html) - su cisco.com
[2] (**EN**) http://lcamtuf.coredump.cx/oldtcp/tcpseq.html
[3] (**EN**) http://lcamtuf.coredump.cx/newtcp/
[4] (**EN**) http://www.monkey.org/~dugsong/dsniff/- Sito ufficiale di dsniff
[5] (**EN**) http://ettercap.sourceforge.net/- Sito ufficiale di Ettercap

Voci correlate

- Rete (informatica)
- Accesso abusivo ad un sistema informatico o telematico
- MAC spoofing

SQL injection

In informatica la **SQL injection** è una tecnica dell'hacking mirata a colpire le applicazioni web che si appoggiano su un database di tipo SQL. Questo exploit sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL. Le conseguenze prodotte sono imprevedibili per il programmatore: l'SQL injection permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito anche senza essere in possesso delle credenziali d'accesso e di visualizzare e/o alterare dati sensibili.

Applicazione pratica

Per un esempio pratico ricorreremo ad uno script in PHP[1] che si appoggia ad un database MySQL. La tecnica che è alla base dell'SQL injection è comunque identica anche per altri tipi di namedatabase o di linguaggio (come l'ASP). Lo script utilizzato come esempio si occupa di autenticare un utente ed è diviso in due file: il primo è *form.html* (un semplice form per il login in HTML), il secondo *login.php* (che controllerà i dati e stabilirà, se consentito, il login. È in PHP). L'utente visualizza *form.html* e compila i dati, che verranno automaticamente inviati a *login.php*, che li memorizza sotto forma di variabile globale *$_POST*.

form.html

```
<form action='login.php' method='post'>
   Username: <input type='text' name='user' />
   Password: <input type='password' name='pwd' />
   <input type='submit' value='Login' />
</form>
```

Il form è molto semplice: ha solo due campi, uno per l'username e uno per la password. I dati immessi verranno poi passati (come detto) a *login.php*, nelle variabili rispettive *$_POST['user']* e *$_POST['pwd']*. Una volta ricevuti questi dati, PHP effettua una query e li cerca all'interno del database. Se verranno trovati procederà all'autenticazione dell'utente.

login.php

```
<font size="12">
<?php

//Prepara la query, in una variabile
$query = "SELECT * FROM users WHERE user='".$_POST['user']."' AND
pwd='".$_POST['pwd']."'";

//Esegue la query (supponiamo che sia già aperta una connessione valida
 al database e $db è lo stato)
$sql = mysql_query($query,$db);

//Conta il numero di righe trovate (se questo numero è maggiore di 0 i
dati immessi sono corretti)
if(mysql_affected_rows($sql)>0)
{
//Esegue la convalida dell'autenticazione e permette l'accesso a pagine
 protette
```

```
}

?>
</font>
```

L'attacco di SQL injection sta proprio nell'iniettare nello script PHP dati arbitrari tramite il form in HTML. In questo caso, se lo script non compie i dovuti controlli, basta immettere per esempio come user **pippo** e come password **' OR user='pippo** per accedere con le credenziali dell'utente *pippo* (ipotizzando l'esistenza dell'utente di nome pippo). La query per il database diventerà infatti:

```
<font size="12">
SELECT * FROM users WHERE user='pippo' AND pwd='' OR user='pippo'
</font>
```

La disgiunzione inclusiva **OR** è uguale al legame logico **VEL** e restituisce TRUE se una delle due condizioni è vera. La condizione per l'utente pippo è verificata e quindi il login viene effettuato.

Proteggersi dalla SQL injection

L'unica possibilità di protezione è un controllo sui dati ricevuti da parte del programmatore, durante lo sviluppo del programma. Bisogna cioè assicurarsi che l'input ricevuto rispetti le regole necessarie, e questo può essere fatto in diversi modi:

- controllare il tipo dei dati ricevuti (se ad esempio ci si aspetta un valore numerico, controllare che l'input sia un valore numerico);
- forzare il tipo dei dati ricevuti (se ad esempio ci si aspetta un valore numerico, si può forzare l'input affinché diventi comunque un valore numerico);
- filtrare i dati ricevuti attraverso le espressioni regolari (regex);
- sostituire i caratteri pericolosi con equivalenti caratteri innocui (ad esempio in entità HTML);
- effettuare l'escape dei dati ricevuti (ogni linguaggio, solitamente, mette a disposizione particolari strumenti per questo scopo, ad esempio `addslashes` e `stripslashes` in PHP, e `PreparedStatement` in Java).
- nel caso del login qui sopra, criptare le credenziali di accesso prima di inserirle nella query SQL (evitare che le informazioni sensibili siano memorizzate nel DB in chiaro).

Ovviamente, questi metodi possono essere applicati anche insieme sullo stesso dato in input. La scelta varia proprio a seconda delle tipologie di questi dati. Occorre, quindi, prestare particolare attenzione a tutte le varianti di un input, tenendo conto di ogni possibile (oppure improbabile) ipotesi.

Note

[1] Si faccia riferimento alla documentazione ufficiale di PHP (http://www.php.net/manual/it/)

Collegamenti esterni

- Proteggersi dall'SQL injection in PHP (http://antirez.com/post/33)
- (**EN**) Un sito guida su come proteggersi in generale dalla SQL injection (http://bobby-tables.com/)
- (**EN**) Blind SQL Injection (http://www.ihteam.net/papers/blind-sqli-regexp-attack.pdf)

Virus (informatica)

Nella sicurezza informatica un **virus** è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di se stesso, generalmente senza farsi rilevare dall'utente (sotto questo punto di vista il nome è in perfetta analogia con i virus in campo biologico). Coloro che creano virus sono detti *virus writer*.

I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano comunque un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

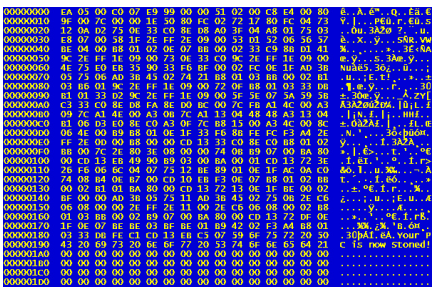
Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di malware, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan, dialer o spyware.

```
push esi
mov edi, sec_roffset                ;copy loader
add edi, fbuffer
mov pcktoffset, edi
ldr_addr esi, loader_start
mov ecx, loader_size
rep movsb
pop esi

mov edx, sec_voffset                ;calculate entrypoint
mov ecx, pe_header
mov ecx, dword ptr [ecx+34h]
add edx, ecx
mov ecx, sec_roffset
add ecx, fbuffer
add ecx, (offset new_oep - offset loader_start)
mov dword ptr [ecx], edx

inf_addr eax, base_ptr
mov eax, dword ptr [eax]
add eax, sec_voffset
add eax, (offset new_oep - offset loader_start)
push eax
inf_addr eax, base_ptr
mov eax, dword ptr [eax]
push eax
push fbuffer
push pe_header
ldr_invoke wrap_apis                ;wrap api calls to run loader
test eax, eax
je infect_file_error
```

Virus che ha infettato un file PE in linguaggio assembly

Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-2007, Award Software, Inc.
Intel P35 BIOS for P35C-DS3R F2a
Memory Runs at Dual Channel Interleaved
Boot Disk failure. Type key to retry
Boot Disk failure. Type key to retryYour PC is now Stoned!
Non-System Disk or disk error
Replace and press any key when ready
Boot Disk Failure. Type key to retry
Boot Disk failure. Type key to retry
Your PC is now Stoned!
<DEL>:BIOS Setup/Q-Flash <F9>:XpressRecovery2 <F12>:Boot Menu <End>:Qflash
05/11/2007-P35-ICH9-6A79UG0BC-00

Stoned (1987)



Stoned Code

Storia

Nel 1949 John von Neumann dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente. Il concetto di programma auto-replicante trovò la sua evoluzione pratica nei primi anni 60 nel gioco ideato da un gruppo di programmatori dei Bell Laboratories della AT&T chiamato "*Core Wars*", nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda. Era l'inizio della storia dei virus informatici.[1]

Il termine *virus* venne adottato la prima volta da Fred Cohen (1984) della University of Southern California nel suo scritto *Experiments with Computer Viruses* (Esperimenti con i virus per computer), dove questi indicò Leonard Adleman come colui che aveva adattato dalla biologia tale termine.
La definizione di virus era la seguente: «Un virus informatico è un programma che ricorsivamente ed esplicitamente copia una versione possibilmente evoluta di sé stesso».[2]

Nel 1972 David Gerrold scrisse un romanzo di fantascienza *La macchina di D.I.O.* (*When H.A.R.L.I.E. was One*), dove è presente una descrizione di un programma per computer chiamato *VIRUS* che adotta il medesimo comportamento di un virus. Nel 1975 John Brunner scrisse il romanzo *Codice 4GH* (*The Shockwave Rider*) in cui

sono descritti programmi chiamati *tapeworms* che si infiltrano nella rete con lo scopo di cancellare tutti i dati. Nel 1973 la frase "virus del computer" era stata usata nel film *Il mondo dei robot (Westworld)*. Il termine *virus del computer* con il significato corrente è inoltre presente anche nell'albo a fumetti *Uncanny X-Men* n. 158, pubblicato nel 1982. Si può dunque affermare che Cohen fece per primo uso della parola virus solo in campo accademico, dato che questa era già presente nella lingua parlata.

Un programma chiamato *Elk Cloner* è accreditato come il primo virus per computer apparso al mondo. Fu creato nel 1982 da Rich Skrenta sul DOS 3.3 della Apple e l'infezione era propagata con lo scambio di floppy disk. Nel corso degli anni ottanta e nei primi anni novanta fu lo scambio dei floppy la modalità prevalente del contagio da virus informatici. Dalla metà degli anni novanta, invece, con la diffusione di internet, i virus ed i cosiddetti *malware* in generale, iniziarono a diffondersi assai più velocemente, usando la rete e lo scambio di e-mail come fonte per nuove infezioni. Il bersaglio preferito di questi software sono prevalentemente le varie versioni di Windows.

Il primo virus informatico famoso nel mondo venne creato nel 1986 da due fratelli pakistani proprietari di un negozio di computer per punire chi copiava illegalmente il loro software. Il virus si chiamava *Brain*, si diffuse in tutto il mondo, e fu il primo esempio di virus che infettava il settore di avvio. [3]

Il primo file infector apparve nel 1987. Si chiamava Lehigh e infettava solo il file *command.com*. Nel 1988 Robert Morris Jr. creò il primo worm della storia. L'anno seguente, nel 1989, fecero la loro comparsa i primi virus polimorfi, con uno dei più famosi: Vienna, e venne diffuso il trojan AIDS (conosciuto anche come Cyborg), molto simile al trojan dei nostri giorni chiamato PGPCoder. Entrambi infatti codificano i dati del disco fisso chiedendo poi un riscatto all'utente per poter recuperare il tutto.[3]

Nel 1995 il primo macrovirus, virus scritti nel linguaggio di scripting di programmi di Microsoft come MS-Word ed Outlook che infettano soprattutto le varie versioni dei programmi Microsoft attraverso lo scambio di documenti. Concept fu il primo macro virus della storia. Nel 1998 la nascita di un altro dei virus storici, Chernobyl o CIH, famoso perché sovrascriveva il BIOS della scheda madre e la tabella delle partizioni dell'hard disk infettato ogni 26 del mese.

La diffusione di massa di Internet nella fine degli anni 90 determina la modifica delle tecniche di propagazione virale: non più floppy ma worm che si diffondono via e-mail. Tra i worm di maggior spicco antecedenti al 2000: Melissa, Happy99 e BubbleBoy, il primo worm capace di sfruttare una falla di Internet Explorer e di autoeseguirsi da Outlook Express senza bisogno di aprire l'allegato.[3]

Nel 2000 il famoso *I Love You* che dà il via al periodo degli script virus, i più insidiosi tra i virus diffusi attraverso la posta elettronica perché sfruttano la possibilità, offerta da diversi programmi come Outlook e Outlook Express di eseguire istruzioni attive (dette *script*), contenute nei messaggi di posta elettronica scritti in HTML per svolgere azioni potenzialmente pericolose sul computer del destinatario. I virus realizzati con gli script sono i più pericolosi perché possono attivarsi da soli appena il messaggio viene aperto per la lettura. *I Love You* si diffuse attraverso la posta elettronica in milioni di computer di tutto il mondo, al punto che per l'arresto del suo creatore, un ragazzo delle Filippine, dovette intervenire una squadra speciale dell'FBI. Era un messaggio di posta elettronica contenente un piccolo programma che istruiva il computer a rimandare il messaggio appena arrivato a tutti gli indirizzi contenuti nella rubrica della vittima, in questo modo generando una specie di catena di sant'Antonio automatica che saturava i server di posta.[4]

Dal 2001 un incremento di *worm* che, per diffondersi, approfittano di falle di programmi o sistemi operativi senza bisogno dell'intervento dell'utente. L'apice nel 2003 e nel 2004: *SQL/Slammer*, il più rapido worm della storia - in quindici minuti dopo il primo attacco Slammer aveva già infettato metà dei server che tenevano in piedi internet mettendo fuori uso i bancomat della Bank of America, spegnendo il servizio di emergenza 911 a Seattle e provocando la cancellazione per continui inspiegabili errori nei servizi di biglietteria e check-in[5]; ed i due *worm* più famosi della storia: *Blaster* e *Sasser*.[3]

Nel giugno 2009 è nata una nuova tipologia di virus che ha come bersaglio sistemi informatici industriali, il primo virus di questa nuova tipologia è stato Stuxnet chi ha preso come mira i sistemi SCADA.

Descrizione

Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni, (da pochi byte ad alcuni kilobyte), ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile. Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto.

Tuttavia, un virus di per sé non è un programma eseguibile, così come un virus biologico non è di per sé una forma di vita. Un virus, per essere attivato, deve infettare un programma ospite, o una sequenza di codice che viene lanciata automaticamente, come ad esempio nel caso dei boot sector virus. La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di sé stesso nel file eseguibile che deve infettare, pone tra le prime istruzioni di tale eseguibile un'istruzione di salto alla prima linea della sua copia ed alla fine di essa mette un altro salto all'inizio dell'esecuzione del programma. In questo modo quando un utente lancia un programma infettato viene dapprima impercettibilmente eseguito il virus, e poi il programma. L'utente vede l'esecuzione del programma e non si accorge che il virus è ora in esecuzione in memoria e sta compiendo le varie operazioni contenute nel suo codice.

Principalmente un virus esegue copie di sé stesso spargendo l'epidemia, ma può avere anche altri compiti molto più dannosi (cancellare o rovinare dei file, formattare l'hard disk, aprire delle backdoor, far apparire messaggi, disegni o modificare l'aspetto del video, ...)

Componenti di un virus

I virus informatici più semplici sono composti da due parti essenziali, sufficienti ad assicurarne la replicazione:

- una *routine di ricerca*, che si occupa di ricercare dei file adatti ad essere infettati dal virus e controlla che gli stessi non ne contengano già una copia, per evitare una ripetuta infezione dello stesso file;
- una *routine di infezione*, con il compito di copiare il codice virale all'interno di ogni file selezionato dalla routine di ricerca perché venga eseguito ogni volta che il file infetto viene aperto, in maniera trasparente rispetto all'utente.

Molti virus sono progettati per eseguire del codice estraneo alle finalità di replicazione del virus stesso e contengono dunque altri due elementi:

- la *routine di attivazione*, che contiene i criteri in base ai quali il virus decide se effettuare o meno l'attacco (es. una data, o il raggiungimento di un certo numero di file infetti);
- il *payload*, una sequenza di istruzioni in genere dannosa per il sistema ospite, come ad esempio la cancellazione di alcuni file o la visualizzazione di messaggi sullo schermo.

I virus possono essere criptati e magari cambiare algoritmo e/o chiave ogni volta che vengono eseguiti, quindi possono contenere altri tre elementi:

- una *routine di decifratura*, contenente le istruzioni per decifrare il codice del virus;
- una *routine di cifratura*, di solito criptata essa stessa, che contiene il procedimento per criptare ogni copia del virus;
- una *routine di mutazione*, che si occupa di modificare le routine di cifratura e decifratura per ogni nuova copia del virus.

Modalità di diffusione

Ciò che distingue i virus propriamente detti dai worm è la modalità di replicazione e di diffusione: un virus è un frammento di codice che non può essere eseguito separatamente da un programma ospite, mentre un worm è un applicativo a sé stante. Inoltre, alcuni worm sfruttano per diffondersi delle vulnerabilità di sicurezza, e non dipendono quindi dal fatto di ingannare l'utente per farsi eseguire.

Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di diffusione dei virus da una macchina ad un'altra era lo scambio di floppy disk contenenti file infetti o un virus di boot. Il veicolo preferenziale di infezione è invece oggi rappresentato dalle comunicazioni e-mail e dalle reti di peer to peer (ad esempio eMule).

Nei sistemi informatici Windows è di consuetudine usare il registro di sistema per inserire in chiavi opportune dei nuovi programmi creati ad hoc dal programmatore di virus che partono automaticamente all'avvio. Uno dei punti deboli del sistema Windows è proprio il suo registro di configurazione. Esistono vari programmi per tenere d'occhio le chiavi pericolose del registro di Windows, uno di questi è Absolute Startup, che ad intervalli di tempo regolari esegue una scansione delle zone a rischio del registro per vedere se un nuovo virus o programma anomalo è stato aggiunto in quelle chiavi.

Ciclo di vita di un virus

I virus informatici presentano numerose analogie con quelli biologici per quello che riguarda il ciclo di vita, che si articola nelle fasi seguenti:

- *creazione*: è la fase in cui lo sviluppatore progetta, programma e diffonde il virus. Di solito i cracker per la realizzazione di virus utilizzano linguaggi di programmazione a basso livello (quali l'assembler e C) in modo da ottenere codice virale di pochi centinaia di byte. La diffusione di pacchetti software che permettono anche ad utenti inesperti di creare virus pericolosissimi ha reso accessibile il procedimento di creazione anche a persone senza competenze.
- *incubazione*: il virus è presente sul computer da colpire ma non compie alcuna attività. Rimane inerte fino a quando non si verificano le condizioni per la sua attivazione;
- *infezione*: il virus infetta il file e di conseguenza il sistema
- *attivazione*: al verificarsi delle condizioni prestabilite dal cracker, il virus inizia l'azione dannosa.
- *propagazione*: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi
- *riconoscimento* (in alcuni casi questa fase non inizia): il virus viene riconosciuto come tale e viene individuata la stringa di riconoscimento, ossia la firma che contraddistingue ciascun virus
- *estirpazione*: è l'ultima fase del ciclo vitale del virus. Il virus viene eliminato dal sistema.[6]

Criteri di classificazione dei virus

I virus informatici possono essere suddivisi in categorie in base alle seguenti caratteristiche:

- ambiente di sviluppo
- capacità operative degli algoritmi
- capacità distruttive.

Esistono poi combinazioni delle categorie precedenti: ad esempio vi sono virus che sono contemporaneamente file virus e boot virus. In tal caso il loro algoritmo di infezione è più complesso potendo eseguire attacchi differenti.[7]

Ambiente di sviluppo

I virus si sviluppano su diversi supporti fisici e per questo sono classificabili in:

- *file virus*, che a loro volta si dividono in:
  - parasitic virus;
  - companion virus;
  - virus link;* *boot virus*;
- *macro virus*;
- *network virus*

Si possono incontrare anche nei giochi download come 4Story, Cabal ecc Spesso ci sono stati utenti che hanno riscontrato particolari problemi di annidamento di virus nella cache di Java.

Capacità operative degli algoritmi

In base alle caratteristiche dei loro algoritmi, i virus si distinguono in:

- *TSR virus*;
- *virus polimorfi*;
- *stealth virus*

In generale non esistono molti virus informatici che sono solo stealth, polimorfici o TSR, perché sarebbero facilmente individuabili. In realtà i computer virus sono formati da una combinazione dei precedenti.

Capacità distruttive

A seconda del tipo di danni causati, i virus si classificano in:

- *innocui*: se comportano solo una diminuzione dello spazio libero sul disco senza nessun'altra alterazione delle operazioni del computer;
- *non dannosi*: se comportano solo una diminuzione dello spazio libero sul disco, col mostrare grafici, suoni o altri effetti multimediali.
- *dannosi*: possono provocare problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file);
- *molto dannosi*: Causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco).

Sintomi più frequenti di infezione

- *Rallentamento del computer*: il computer lavora molto più lentamente del solito. Impiega molto tempo ad aprire applicazioni o programmi. Il sistema operativo impiega molto tempo ad eseguire semplici operazioni che solitamente non richiedono molto tempo[8];
- *Impossibilità di eseguire un determinato programma o aprire uno specifico file*;
- *Scomparsa di file e cartelle*: i file memorizzati in determinate cartelle (di solito quelle appartenenti al sistema operativo o a determinate applicazioni) sono scomparse perché cancellate dal virus. Potrebbero scomparire intere directory;
- *Impossibilità di accesso al contenuto di file*: all'apertura di un file, viene visualizzato un messaggio di errore o semplicemente risulta impossibile aprirlo. Un virus potrebbe aver modificato la File Allocation Table (FAT) provocando la perdita degli indirizzi che sono il punto di partenza per la localizzazione dei file;
- *Messaggi di errore inattesi o insoliti*: visualizzazione di finestre di dialogo contenenti messaggi assurdi, buffi, dispettosi o aggressivi;

- *Riduzione di spazio nella memoria e nell'hard disk*: riduzione significativa dello spazio libero nell'hard disk; quando un programma è in esecuzione, viene visualizzato un messaggio indicante memoria insufficiente per farlo (sebbene questo non sia vero e ci siano altri programmi aperti);
- *Settori difettosi*: un messaggio informa della esistenza di errori nella parte di disco sulla quale si sta lavorando e avverte che il file non può essere salvato o che non è possibile eseguire una determinata operazione;
- *Modifiche delle proprietà del file*: il virus modifica alcune o tutte le caratteristiche del file che infetta. Di conseguenza risultano non più corrette o modificate le proprietà associate al file infettato. Tra le proprietà più colpite: data/ora (di creazione o dell'ultima modifica), la dimensione;
- *Errori del sistema operativo*: operazioni normalmente eseguite e supportate dal sistema operativo determinano messaggi di errore, l'esecuzione di operazioni non richieste o la mancata esecuzione dell'operazione richiesta;
- *Duplicazione di file*: se ci sono due file con lo stesso nome ma con estensione rispettivamente EXE e COM, quello con estensione COM sarà un virus. I virus fanno così perché in caso di presenza di due file con lo stesso nome il sistema operativo eseguirà sempre per primo quello con estensione COM;
- *Ridenominazione di file*: un virus può rinominare i file infettati e/o file specifici;
- *Problemi di avvio del computer*: il computer non si avvia o non si avvia nella solita maniera;
- *Blocchi del computer*: nonostante l'apertura di pochi o nessun programma e la mancanza di un pesante carico sul sistema, questo si blocca ("crasha"), rendendo necessario l'utilizzo del Task Manager per rimuovere il task bloccato o riavviare il computer;
- *Interruzione del programma in esecuzione* senza che l'utente abbia eseguito operazioni inaspettate o fatto qualcosa che potrebbe aver provocato questo risultato;
- *Apertura e chiusura del lettore CD/DVD* senza intervento dell'utente;
- *Tastiera e/o mouse non funzionanti correttamente*: la tastiera non scrive ciò che è digitato dall'utente o esegue operazioni non corrispondenti ai tasti premuti. Il puntatore del mouse si muove da solo o indipendentemente dal movimento richiesto dall'utente;
- *Scomparsa di sezioni di finestre*: determinate sezioni (pulsanti, menu, testi etc…) che dovrebbero apparire in una particolare finestra sono scomparse o non vengono visualizzate. Oppure, in finestre nelle quali non dovrebbe apparire nulla, appaiono invece icone strane o con contenuto insolito (ad esempio nella taskbar di Windows;
- *Riavvio spontaneo del computer*;
- *Antivirus disattivato automaticamente*;
- *Programmi all'improvviso non più funzionanti o malfunzionanti*;
- *Lentezza della connessione Internet*;
- *Emissione da parte del computer di suoni insoliti*;
- *Microsoft Internet Explorer si blocca o comunque funziona male* dando continui errori (ad esempio non riesce a chiudere la finestra delle applicazioni)

Si tenga comunque presente che i sintomi appena descritti potrebbero essere riconducibili a cause diverse da virus. Nel caso di presenza di uno o più di questi sintomi, è comunque consigliabile l'esecuzione di una scansione antivirus del sistema;

Tecniche usate per il rilevamento di virus

Non esiste un metodo generale per individuare un virus all'interno di un sistema. Le tecniche di rilevamento utilizzate dagli antivirus sono diverse: utilizzate contemporaneamente garantiscono un'ottima probabilità di rilevamento della presenza di un virus. In base alle tecniche di rilevamento usate, gli antivirus si distinguono in tre tipi:

- *programmi di monitoraggio*:mirano a prevenire un'infezione mediante il controllo di attività sospette (ad esempio, la richiesta di formattazione di un disco oppure l'accesso a zone privilegiate di memoria). Sono importanti perché rappresentano la prima linea di difesa. Ma sono facili da bypassare attraverso la tecnica di tunnelling.
- *scanner*: effettuano la ricerca dei virus attraverso due tecniche:
  - il confronto tra le firme memorizzate in un database interno, con quelle, eventualmente, contenute nei file infetti;
  - l'utilizzazione delle tecniche euristiche per i virus che sono cifrati o sconosciuti.
- *programmi detection*: utilizzano due tecniche:
  - verifica dell'integrità: calcolano l'hash dei file da confrontare successivamente coi nuovi valori risultanti da un nuovo calcolo per verificare che i file non abbiano subito modifiche nel frattempo.
  - tecniche euristiche: salva le informazioni sufficienti per ripristinare il file originale qualora questo venga danneggiato da un virus.[9]

Virus ieri ed oggi

Oggi sono ben pochi i codici malevoli ai quali si può attribuire, propriamente, il nome di virus. Quando un tempo lo scambio dei file avveniva tramite supporti fisici, generalmente i floppy, erano questi ad essere veicolo delle infezioni e pertanto era importante, volendo creare un virus che si diffondesse, che questo fosse il più silenzioso possibile. Venivano scritti in assembly e questo li rendeva piccoli, performanti ed insidiosi seguendo la regola: se non sai cosa cercare figurati se sai come trovarlo.

Parlando oggi di virus, entrando nel particolare, si commette però un errore. Si intende quindi, con il termine virus, tutto il codice malevolo in grado di arrecare danno ad un utente. Lo scambio di file tramite dispositivi fisici quali il floppy, il quasi totale abbandono degli stessi per effettuare una procedura di boot e di ripristino, ha reso obsoleto il vecchio concetto di virus, un piccolo codice malevolo difficile da individuare. Nondimeno le macchine sono sempre più performanti, gli utenti sempre di più e sempre meno preparati, la banda larga per tutti. Le informazioni viaggiano da un capo all'altro del pianeta senza vincoli fisici ormai, e così anche il codice malevolo.

Il vecchio concetto di virus è stato sostituito con quello più moderno di worm. I worm non sono più scritti in assembly ma in linguaggi di programmazione di livello sempre più alto in stretta connivenza con il sistema operativo, nella quasi totalità dei casi Windows, e le sue vulnerabilità. Tutto questo rende la stesura di un codice malevolo molto più semplice che in passato ed il gran numero e la diversità di worm con rispettive varianti ne è un esempio lampante. Questi nuovi tipi di infezioni penetrano nel sistema quasi sempre da soli sfruttando le vulnerabilità, non fanno molto per nascondersi, si replicano come vermi anziché infettare i file, che è un'operazione più complessa ed ormai in disuso.

Ultimamente vanno molto di moda payload altamente distruttivi o che espongono la vittima ad altri tipi di attacchi. La vita dei worm è generalmente più breve di quella di un virus perché identificarlo, grazie ad internet, è diventato un business ora più grande che in tempi passati ed è probabilmente questo che porta sempre più spesso gli ideatori a voler un ciclo di vita più breve anche per la macchina che lo ospita e qualche capello in meno all'utente. I worm agiscono sempre più spesso come retrovirus e, volendo correre più veloce delle patch che correggono le vulnerabilità che ne hanno permesso la diffusione, spesso ci si trova ad aggiornare l'antivirus quando il codice ha già preso piede nel sistema.

Scambio di virus

Molti programmatori di virus ai nostri giorni, ma soprattutto nel passato, si sono scambiati sorgenti di virus per capire nuove tecniche di programmazione. Molti scambi di virus sono avvenuti tramite siti web chiamati *VX*. *VX* significa Virus eXchange. Al giorno d'oggi i siti (almeno quelli pubblici) dedicati al VX sono rimasti pochi ma si pensa che esistano dei siti underground che contengano dei database di virus recenti accessibili solo a crew virus writer. Si possono ricevere virus anche attraverso mail, che installano il virus anche se non vengono aperte.

Falsi virus

La scarsa conoscenza dei meccanismi di propagazione dei virus e il modo con cui spesso l'argomento viene trattato dai mass media favoriscono la diffusione tanto dei virus informatici quanto dei virus burla, detti anche hoax: sono messaggi che avvisano della diffusione di un fantomatico nuovo terribile virus con toni catastrofici e invitano il ricevente ad inoltrarlo a quante più persone possibile. È chiaro come questi falsi allarmi siano dannosi in quanto aumentano la mole di posta indesiderata e diffondono informazioni false, se non addirittura dannose.

I virus in Linux

In Linux, ad oggi non c'è stata una grandissima diffusione di virus in quanto grazie al meccanismo dei permessi dei sistemi multiutente a cui Linux appartiene, le infezioni si limitano esclusivamente all'utente che possiede il file infetto con un impatto sull'intero sistema estremamente ridotto.

Uno dei primi virus (un trojan per la precisione) per Linux, di nome Bliss[10], doveva infatti essere installato ed essere eseguito in modalità superutente (root). L'hacker britannico Alan Cox lo definì "un giocattolo".

Altre minacce informatiche

All'inizio tutte le minacce informatiche erano virus come sopra definiti, successivamente sono comparse e si sono specializzate diverse altre minacce, anche se nel linguaggio comune continuano impropriamente ad essere chiamate "virus informatici":

Backdoor
: o "porta di servizio"; punto di passaggio attraverso il quale si può prendere il controllo di un computer.

Buffer overflow
: tecnica per inviare dati di lunghezza superiore a quella programmata per oltrepassare la capacità del buffer.

DoS e la sua variante DRDoS
: "negazione del servizio"; tecnica per tempestare di richieste un singolo servizio al fine di farlo collassare.

Exploit
: tecnica per prendere il controllo di un computer sfruttando le debolezze (bug) del sistema operativo o di altri programmi che accedono ad Internet.

Ingegneria sociale
: tecnica di studio di un bersaglio per carpirne la fiducia ed entrarne in contatto.

Keylogger
: software che una volta eseguito su di una macchina memorizza in maniera trasparente all'utente ogni tasto premuto in un proprio database. Solitamente viene installato tramite virus o backdoor, e viene programmato in modo che ritrasmetta via rete i dati memorizzati.

Phishing
: tecnica di ingegneria sociale per ottenere informazioni riservate al fine del furto di identità e di informazioni personali.

Port scanning

tecnica per verificare lo stato (accepted, denied, dropped, filtered) delle 65.535 porte (socket) di un computer.

Rootkit

programmi che permettono ai virus di "nascondersi" nel computer.

Sniffing

o "annusare"; tecnica per intercettare i dati in transito in rete e decodificarli.

Trojan Horse

o "cavallo di Troia" sono genericamente software malevoli (malware) nascosti all'interno di programmi apparentemente utili, e che dunque l'utente esegue volontariamente. Il tipo di software malevolo che verrà silenziosamente eseguito in seguito all'esecuzione del file da parte dell'utente può essere sia un virus che un qualunque tipo di minaccia informatica poiché permette al cracker che ha infettato il PC di risalire all'indirizzo IP della vittima.

Wardialing

uso di un modem con il fine di chiamare ogni possibile telefono in una rete locale per trovare un computer assieme alle varianti Wardriving e Warflying.

Note

[1] *Sicurezza: virus, worm, trojan...* (http://www.bloomriot.org/91/sicurezza-virus-worm-trojan.html), www.bloomriot.org.
[2] *Breve storia dei virus informatici* (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_2.html), www.hwupgrade.it.
[3] *Breve storia dei virus informatici* (http://www.hwupgrade.it/articoli/sicurezza/1424/virus-e-antivirus-l-eterna-lotta-fra-il-bene-e-il-male_3.html), www.hwupgrade.it.
[4] *"I love you": un virus targato Microsoft* (http://www.questotrentino.it/2000/11/I_love_you.htm), www.questotrentino.it.
[5] *Anche il virus ha un lato buono* (http://mobile.ilsole24ore.com/solemobile//esplosonews.jsp?uuid=cbbb3d5a-b6e1-11dd-bb4d-604737b5fe8c), Il Sole 24ore.com.
[6] *ciclo di vita di computer virus* (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/), www.dia.unisa.it.
[7] *classificazione computer virus* (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/classificazione.htm), www.dia.unisa.it.
[8] *Quali sono i sintomi per riconoscere se ho preso un virus?* (http://pchelp-howto.blogspot.com/2008/07/quali-sono-i-sintomi-per-riconoscere-se.html), pchelp-howto.blogspot.com.
[9] *Tecniche usate per il rilevamento di computer virus* (http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/virus/), www.dia.unisa.it.
[10] (http://math-www.uni-paderborn.de/~axel/bliss/alan_analysis.txt)

Voci correlate

- Malware
- Macrovirus
- Trojan
- Spyware
- Antivirus

Altri progetti

- **Wikimedia Commons** contiene file multimediali: http://commons.wikimedia.org/wiki/Category:Computer viruses

Collegamenti esterni

- (EN) VX Heavens (http://vx.netlux.org/) sito con database e sorgenti di migliaia di virus.

Warez

Warez è un termine in gergo informatico che indica materiale, prevalentemente software, distribuito in violazione al copyright che lo ricopre.

Storicamente il termine non è associato ad alcuno scopo di lucro, quanto piuttosto di perdita di profitto per il mancato acquisto del prodotto informatico: la vendita non è caratteristica del Warez. Solitamente ci si riferisce a distribuzioni di software ad opera di gruppi organizzati e limitatamente alla cerchia di amici e conoscenti o utenti con i medesimi interessi, in contrapposizione con le reti peer-to-peer. Le origini del termine risalgono ai primi circoli underground di appassionati di computer che si scambiavano programmi attraverso le BBS e, da allora, si è evoluto fino ad indicare uno o più software rilasciati illegalmente (da cui la forma plurale di *(soft)**wares*** distorta con carattere lievemente dispregiativo in ***warez***). In lingua inglese, *warez* è utilizzato come sostantivo o come verbo. Le persone che distribuiscono warez sono indicati come *pirati informatici*, mentre coloro che rimuovono le protezioni del software sono noti come *cracker*. Solitamente sono i *cracker* i primi a diffondere in rete il software che hanno illegalmente modificato; probabilmente, ciò è la ragione per la quale sono conosciuti piuttosto col nome di *pirati informatici* e per cui nel gergo comune si è diffuso tal termine, a dispetto di quello di *cracker*, relativamente poco usato e spesso erroneamente confuso con quello di *hacker*.

Ultimamente il Warez è sempre più associato al concetto di lucro, a causa dei numerosi siti internet che offrono collegamenti a download illegali, previo pagamento di un compenso. In altri casi non è richiesta alcuna forma di pagamento diretta, ma il lucro deriva dall'utilizzo di forme di pubblicità invasiva, talvolta anche di tipo virale. Un rischio per l'utente che ricerca materiale di questo tipo è costituito dai cosiddetti siti warez civetta: il download effettuato non contiene il programma scelto, bensì varietà di trojan, malware e worm. Lo scopo è alimentare le oramai vaste botnet, usate per vari scopi illeciti. Molto spesso i pirati informatici ricorrono ai motori di ricerca più comuni (Google.com ecc...) per trovare CRACK, PATCH, KEY GENERATOR, SERIAL, TRIAL RESET O FULL PROGRAMS, linguaggio molto comune usato spesso in rete per trovare file che riescono ad *ingannare* il programma facendogli credere di aver già acquistato la versione completa di un programma a pagamento...

Voci correlate

- Twilight (CD-ROM)

Fonti e autori delle voci

Cracker *Fonte*: http://it.wikipedia.org/w/index.php?oldid=54161571 *Autori:*: .anaconda, Abisys, Acolleoni, AmonSûl, Aplasia, Archenzo, Ary29, AttoRenato, Avesan, Azrael555, Bultro, CavalloRazzo, Ciampix, Crackeranonymous, Cruccone, Daniele Pugliesi, DarkAsd, Dega180, Drugonot, Duskdruid, Frieda, Gacio, Generale Lee, Guidomac, Habib7, Hellis, Iron Bishop, Kar.ma, Lastknight, Lornova, Luisa, Manny86, Marcel Bergeret, Marcok, Mastervb, Mizardellorsa, Mox83, Nuno Tavares, Osk, Pierosuper, Rael, SUPER KONG, Sannita, Senpai, Sirabder87, Sockpuppet, Taueres, Template namespace initialisation script, Tia solzago, Ticket 2010081310004741, Valhalla, Wikipedia Express, Yerul, 64 Modifiche anonime

Cracking (informatica) *Fonte*: http://it.wikipedia.org/w/index.php?oldid=51371566 *Autori:*: Abisys, Alfio, AttoRenato, Avesan, Bultro, Caig, Daniele Pugliesi, Dega180, Devis, Dome, Drugonot, Granzotto, Jacklab72, Lory2k, Marcok, Marius, No2, Paginazero, Salvatore Ingala, Sbisolo, Vittorioolivati, Zeuslnx, ZioNicco, 10 Modifiche anonime

Crimine informatico *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55452177 *Autori:*: AXRL, Achillu, Andreamonti, Bultro, Daniloviz, Eumolpo, F.delu, Fale, Frigotoni, IlarioGelmetti, Italo da b, Jalo, M7, Massimiliano Lincetto, Massimiliano Panu, Romero, Shivanarayana, Snowdog, 15 Modifiche anonime

Defacing *Fonte*: http://it.wikipedia.org/w/index.php?oldid=54178293 *Autori:*: .anaconda, Abisys, Alessiox.94, Alleborgo, Arepo, Ask21, Avesan, Broc, ColdShine, Elwood, Kar.ma, Kormoran, Marcok, McJavaX, Mda, Melkor II, Mizardellorsa, Moongateclimber, No2, Paginazero, Pietrodn, Remo Mori, Senpai, Snowdog, VincenzoX, 15 Modifiche anonime

Exploit *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55465257 *Autori:*: Abisys, Alez, Andreaf83, Avesan, Caterpillar86, CavalloRazzo, FrAnCiS, Igodeb, Marco C, MaxDel, Melknix, Piero, RaminusFalcon, Ripepette, Rollopack, Salvatore Ingala, Stefano-c, Ticket 2010081310004741, VincenzoX, Yerul, 23 Modifiche anonime

Guerra cibernetica *Fonte*: http://it.wikipedia.org/w/index.php?oldid=52924286 *Autori:*: Abisys, Avesan, Filippof, Gennaro.manna, Hamed, Jalo, Marcok, Neq00, Nickel Chromo, No2, Pracchia-78, Sentruper, Zerosei, 18 Modifiche anonime

Hacker *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55908282 *Autori:*: .anaconda, .mau., Abisys, Adelchi, Agavasan, Alec, Aleksander Sestak, AlessioMela, Alt-os, AmonSûl, Andrea Monaco, Andreabont, Aplasia, Arturo.dicorinto, Aschoo, Austro, Avesan, Balubino, Barbaking, BerserkerWelding, Blakwolf, BrC, Brownout, Buggia, Buzzbomber, Calabash, Carlo.Ierna, Carlogubitosa, CarmineXX, Caulfield, CavalloRazzo, Chesce, Ciampix, Civvì, Claudio Pellegrino, Conocybe, Corinne89, Cosissimo, Davide, Davide21, Dersonlwd, Dinwath, Dirittoinformatico, Djechelon, Dr Zimbu, Dragoonfire34, Drugonot, Earendel, El Demiurgo, Elbloggers, Ernesthedandy, Ezio danise, F. Cosoleto, Fedeg93, Fedesanfi, FiloMJ, Flippo, Fmartorana, Frazzone, Fredericks, Frieda, Ft1, GBG, Gabriele91, Gacio, Giacomo Ritucci, GinkyBiloba, Gionnico, Giovannigobbin, Giukrim84, Gostwriter, Gpx, Guidomac, Hacker2000, Hacklio, Hashar, Helios, Hellis, Homer, Ilario, Ines, Iron Bishop, Jacopo, Jaqen, Joe, Johnlong, Jstevie, Kaiserxol, Kappa14, Kenobiswc, KinG-LioN, Klaudio, Lab, Larry.europe, Laurentius, LoRdHaCk, Looris, Lornova, LucAndrea, Luca330, Lucas, Luisa, M7, Madowiki, Magnum87, MapiVanPelt, Maquesta, Marcok, Marcol-it, Marius, Mark91, Massimiliano Lincetto, Mastervb, Maxx1972, Mercuri88, Midnight bird, Mikosky, MikyT, Mirceaeliade, MoraRossa, Moro, Moroboshi, Mrbeddo, Murdercode, NI-kcarC, Nadira, Nemsix, NewLibertine, Nicoli, Nubifer, Ottomano, Paginazero, Pap3rinik, Pava, PersOnLine, Petrik Schleck, Phantomas, Piero, Pierosuper, Pigr8, Pot, Raynox, Rebek, Remo Mori, Restu20, Riccardov, Ripepette, Rojelio, Rollopack, Rootline, Rossi46GO, Salento81, Sannita, Sassospicco, Sbisolo, Seics, Senpai, Sentruper, Senza nome.txt, Severance, Shivanarayana, Simona85, Simone, Simone003, SkY`, Sky, Snowdog, SpectraOwna, Spock, Stebevice, Stefano Careglio, Suisui, Supradyn, Tanonero, Tarlisky, Taueres, The Fish, Ticket 2010081310004741, TierrayLibertad, Torsolo, Triquetra, Trixt, Twice25, Under, Updown, Vadik, Valepert, Vferrari, Victoria, VincenzoDiMassa, Vituzzu, Weping, Whitedonkey, Wiso, Yerul, Zack Tartufo, 434 Modifiche anonime

Hacktivism *Fonte*: http://it.wikipedia.org/w/index.php?oldid=51011672 *Autori:*: %Pier%, Abisys, Annuale, Arturo.dicorinto, Bramfab, Danilo, Pakdooik, Pracchia-78, Sax123, Texcarson, ZioNicco, 2 Modifiche anonime

Malware *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55961508 *Autori:*: Andre Engels, AndreaFox, Archangelsk, Archenzo, Arf, Asdalol, Avesan, B3t, Buggia, Chiavarus, Doc.mari, Dome, Dr Zimbu, Dr.Gabriel, Emile234topsec, Eumolpo, Formica rufa, Frack, GilliamJF, Gimli, Hashar, Hellis, Malemar, Marcok, Moongateclimber, Morgandy, Mr. Gabry's, Nemo bis, No2, Oile11, Orso della campagna, Paulatz, PersOnLine, Pickblack, Seics, Suisui, Syrio, Truman Burbank, Twice25, Vituzzu, Yerul, 75 Modifiche anonime

Pharming *Fonte*: http://it.wikipedia.org/w/index.php?oldid=51045010 *Autori:*: Archangelsk, Avesan, Daniele Pugliesi, Marcok, Marcuscalabresus, Paginazero, Pietrodn, Pignola, 11 Modifiche anonime

Phishing *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55465295 *Autori:*: A.C.95, Abisys, Aggiailamica, Avesan, Bella Situazione, Beta16, Blakwolf, Bruno Settimo, CristianCantoro, Daniele Pugliesi, Dg, Dirittoinformatico, Eumolpo, Feedbach, Frieda, Gac, Guidomac, Hellis, Hrundi V. Bakshi, Il dalfo, Kabelsalat, KrovatarGERO, Lastknight, LeFilsDePascal, Leitfaden, Luisa, M7, Marco Perticarini, Marcok, Mark91, Massimiliano Lincetto, Megoras, Melefabrizio, Michele.gazzola, Moroboshi, Nanduzzo, No2, Numberinn, Paganinip, Petrik Schleck, Pietrodn, Quasimed, RL, Rupertsciamenna, Salvatore Ingala, Sbisolo, Shivanarayana, Simonefrassanito, Sir marek, Ticket 2010081310004741, Tomfox, Wiso, Ylebru, 126 Modifiche anonime

Script kiddie *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55425883 *Autori:*: Abisys, Akbg, Andy61, Archenzo, Ary29, Avesan, Blakwolf, CavalloRazzo, Cotton, Elninopanza, Ernesthedandy, Eumolpo, Fakk, Filnik, Freepenguin, Fstefani, Ggonnell, Gpx, Gspinoza, Hellis, Jackie, Jacopo Werther, Lornova, Lucazorzi, MapiVanPelt, Marcok, MartinBk, Massic80, Meirut, MikyT, Motumboe, Mox83, Mykelyk, Paolina85, Pop killer, Quatar, Rael, Robertiki, Salento81, Salvatore Ingala, Toobaz, 41 Modifiche anonime

Sicurezza informatica *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55459397 *Autori:*: .anaconda, Acolleoni, Agatino Grillo, Aldolat, Alfio, Andrea Cioffi, Andreaf, AnjaManix, Aquatech, Ask21, Avesan, Azrael555, BMF81, Basilicofresco, Beechs, Bultro, Buzz lightyear, Caesar 808, Calabash, Calibro, Centrodiurnomilano, Cerrigno, Claudio.Pirelli, Condor33, Daniele Pugliesi, Daphiel, Dario Crivello, Davide.it, Dj ture, Elwood, Emilio2005, Eumolpo, Fabio.gastone, Fabry23, Fire90, G84, Gac, Gianfranco, Guidomac, Hellis, Ilbellodelweb999, Jramio, Keledan, LapoLuchini, LaseriumFloyd, Llorenzi, M7, Mac9, Mainframe, Marcok, Maurinap, Maurizio.Cattaneo, Maurooo, Melos, Microsoikos, Mizardellorsa, Nicoli, No2, Paganinip, Panairjdde, Perteghella, Phantomas, PieroT82, Pontiniaweb, Remo Mori, Rh, Riccardov, Rob-ot, Rojelio, Sbisolo, Scorp, Sentruper, Snowdog, Sockpuppet, Superchilum, Ticket 2010081310004741, Tio Sam, Tomford, Truman Burbank, Urashimataro, Vituzzu, 132 Modifiche anonime

Sniffing *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55741768 *Autori:*: 213-156-56-135.fastres.net, Abisys, Amtitti, Ancem, Aplasia, Ary29, AttoRenato, Avesan, Dany3R9, Eumolpo, Fabrizio Tarizzo, Finn81, Gianfranco, Guignol, Hauteville, Hce, Ignlig, Ilgiurista, Incola, Ippatsu, Iron Bishop, Jacopo Werther, Jeankhan, MF, Marcok, Niculinux, No2, Phantomas, Salvatore Ingala, Sbisolo, Senza nome.txt, Shivanarayana, Snowdog, Spikey, Spikeyrock, Tommaso Ferrara, Virnupok, Vituzzu, 40 Modifiche anonime

Spam *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55599979 *Autori:*: .anaconda, .jhc., 213.21.175.xxx, Abisys, Alessio, Alessio Ganci, Alkalin, Amux, Ansgarius, ArmandoEdera, Ary29, Avesan, Beard, Beta16, Biopresto, Bohtont, Bravi Massimiliano, Buggia, Calabash, Caulfield, Cerume, ColdShine, Cruccone, Cyberuly, DarkAp, DarkBeam, Davide.mula, Dedda71, Dome, El Nick, Elbloggers, Eth000, F l a n k e r, F. Cosoleto, Frieda, Furriadroxiu, Gabriel24, Gac, Gacio, Guidomac, Harlock81, Hauteville, Hellis, Ieio78, Ignlig, IlSignoreDeiPC, Iron Bishop, KS, Kahless, Kibira, Kill off, Kronos, Laurentius, Lbreda, Lilja, Limonadis, Lisergia, LoStrangolatore, Looka, Lord Possum, Loroli, LucAndrea, LucaLuca, LuigiPetrella, Luisa, M7, Magnum87, MaiDireChiara, Marchack, Marcok, Marcol-it, MatriX, Maurice Carbonaro, Max98, Melos, Midnight bird, Minucc, Mizardellorsa, Moongateclimber, Nicoli, Ninja, No2, Pablomoroe, Paginazero, Pallanzese, Paul Gascoigne, Phantomas, Piero Montesacro, Pierosuper, Pracchia-78, Rachele.zanchetta, Rael, Ricce, Rollopack, Salvatore Ingala, Sbisolo, Segnali dallo spazio, Senpai, Shanpu, Shivanarayana, Sid-Vicious, Smèagol, Snowdog, Sparko, Square87, Supernino, Taueres, Ticket 2010081310004741, Ticket OTRS 2011102410007641, Tomfox, Tommaso Ferrara, Torredibabele, Trixt, Twice25, Ulisse0, Umal, Unriccio, Veneziano, VincenzoX, Vipera, Vituzzu, Wolf, Yoruno, Zandegù, 184 Modifiche anonime

Spoofing *Fonte*: http://it.wikipedia.org/w/index.php?oldid=51529627 *Autori:*: Abisys, AlessioMela, Alez, Avesan, Centrifuga, Gmantua, Guidoz, Guignol, Hakk, Johnlong, M7, Massimiliano Lincetto, Nijeko, Paginazero, RL, Remo Mori, Roghan, Salvatore Ingala, Spikeyrock, TierrayLibertad, Tund3r, Twice25, Vale 1983, Wiso, 48 Modifiche anonime

SQL injection *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55099574 *Autori:*: .anaconda, Abisys, Alec sp, Alez, Alz, Avesan, Fabrymondo, Francesco Betti Sorbelli, Frankthequeen, Gabriele91, Gac, Hellis, Kormoran, Lillololllo, Marcol-it, Mirkop88, No2, Paolociampanella, R00t.ati, Rojelio, Valepert, VincenzoX, Wikit2006, Zandor zz, 32 Modifiche anonime

Virus (informatica) *Fonte*: http://it.wikipedia.org/w/index.php?oldid=55816113 *Autori:*: .anaconda, .jhc., AKappa, Abisys, Agilurfo, Alfio, Alkalin, Andrea Frizza mito, Ary29, Ask21, AttoRenato, Austro, Avesan, Basilero, Bizio, Buzz lightyear, Clamiax, Colom, Cotton, DPW94, DanGarb, Davide, Davidegat, Dedda71, Dixy rose, Djgwala, Dr Zimbu, Dr.Gabriel, Drugonot, Ekerazha, Eumolpo, Eversor, F l a n k e r, Fabio.gastone, FabrizioC87, Gabriel24, Ghoulsnghosts, Gimli, Giovannigobbin, Giucuo2004, Govoch, Guidomac, Gusme, Hce, Hellis, Henrykus, Ignlig, Iron Bishop, Jalo, Johnlong, Kibira, Klaudio, La Corona, LaPizia, LaseriumFloyd, Laurusnobilis, Lbreda, Luisa, Malemar, MapiVanPelt, Maquesta, Marco Bernardini, Marcok, Marcol-it, Marcuscalabresus, Marijuana, Marius, Mark250594, Mark91, Massic80, MikyT, Mitchan, Nanae, Nicoli, Niculinux, No2, Numbo3, Osk, Overflow, P tasso, Paginazero, Pgianpy, Phantomas, Pierosuper, Pil56, Puppybarf, Quatar, Raistolo, Ralf Roletschek, Ramatteo, Razzabarese, Red michael, Riccardo Loi, Ripepette, Sassospicco, Sbisolo, Seics, Senpai, Shivanarayana, Shíl, Sigjlr, Snowdog, Stef Mec, Suisui, Taueres, The Polish, TierrayLibertad, Tompase, TopFuel, Trianam, Valepert, VincenzoX, Vipera, Vituzzu, Zippit, 258 Modifiche anonime

Warez *Fonte*: http://it.wikipedia.org/w/index.php?oldid=54411075 *Autori:*: Abisys, Airuzzo, Al Pereira, AlessioMela, Alkalin, Andylong, AttoRenato, Avesan, Buzzbomber, CavalloRazzo, Eumolpo, Gionnico, Jalo, LoStrangolatore, Luckyz, Læti, Pavek, Piccolomomo, Pil56, Porta seriale, Ras78, Senpai, Ufobm, 24 Modifiche anonime

Fonti, licenze e autori delle immagini

Immagine:Wikisource-logo.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Wikisource-logo.svg *Licenza*: logo *Autori:*: Guillom, INeverCry, Jarekt, MichaelMaggs, NielsF, Rei-artur, Rocket000

Immagine:Wikibooks-logo.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Wikibooks-logo.svg *Licenza*: logo *Autori:*: User:Bastique, User:Ramac et al.

Immagine:Wikinews-logo.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Wikinews-logo.svg *Licenza*: logo *Autori:*: Vectorized by Simon 01:05, 2 August 2006 (UTC) Updated by Time3000 17 April 2007 to use official Wikinews colours and appear correctly on dark backgrounds. Originally uploaded by Simon.

Immagine:Splinderdefaced.png *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Splinderdefaced.png *Licenza*: sconosciuto *Autori:*: .mau., Archeologo

Immagine:glider.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Glider.svg *Licenza*: Public Domain *Autori:*: Eric S. Raymond

Immagine:Stering.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Stering.jpg *Licenza*: BSD *Autori:*: Original uploader was Lamendoluz at en.wikipedia

Immagine:Spacewar!-PDP-1-20070512.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Spacewar!-PDP-1-20070512.jpg *Licenza*: Creative Commons Attribution 2.0 *Autori:*: Joi Ito from Inbamura, Japan

Immagine:Richard Matthew Stallman.jpeg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Richard_Matthew_Stallman.jpeg *Licenza*: GNU Free Documentation License *Autori:*: BrokenSegue, DCEvoCE, Dbenbenn, Durin, Emijrp, Guety, John Vandenberg, Niqueco, Porao, Sj, Solon, Ævar Arnfjörð Bjarmason, 2 Modifiche anonime

Immagine:Commons-logo.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Commons-logo.svg *Licenza*: logo *Autori:*: SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.

Immagine:Wikiquote-logo.svg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Wikiquote-logo.svg *Licenza*: Public Domain *Autori:*: -xfi-, Dbc334, Doodledoo, Elian, Guillom, Jeffq, Krinkle, Maderibeyza, Majorly, Nishkid64, RedCoat, Rei-artur, Rocket000, 11 Modifiche anonime

File:Beast RAT client.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Beast_RAT_client.jpg *Licenza*: Public Domain *Autori:*: V.H.

File:U.S. Navy Cyber Defense Operations Command monitor.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:U.S._Navy_Cyber_Defense_Operations_Command_monitor.jpg *Licenza*: Public Domain *Autori:*: Mass Communications Specialist 1st Class Corey Lewis , U.S. Navy

File:spammed-mail-folder.png *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Spammed-mail-folder.png *Licenza*: GNU General Public License *Autori:*: Ascánder, Bawolff, Jfd34, KAMiKAZOW, LordT, Nixón, RJaguar3, 12 Modifiche anonime

File:Spam with cans.jpeg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Spam_with_cans.jpeg *Licenza*: Creative Commons Attribution-ShareAlike 3.0 Unported *Autori:*: Matthew W. Jackson

File:ASM-Virus.PNG *Fonte*: http://it.wikipedia.org/w/index.php?title=File:ASM-Virus.PNG *Licenza*: Public Domain *Autori:*: Laberkiste, Seldevago, Tb, Trockennasenaffe, WikipediaMaster, 1 Modifiche anonime

File:Stoned-virus-screenshot.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Stoned-virus-screenshot.jpg *Licenza*: Public Domain *Autori:*: kein Autor, da kein Werk

File:Stoned-virus-hexacode.jpg *Fonte*: http://it.wikipedia.org/w/index.php?title=File:Stoned-virus-hexacode.jpg *Licenza*: Public Domain *Autori:*: keiner, da kein Werk

Licenza

Creative Commons Attribution-Share Alike 3.0 Unported
//creativecommons.org/licenses/by-sa/3.0/